



February 2017

CYBERSECURITY

DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely

CYBERSECURITY

DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely

Why GAO Did This Study

Cyber-based intrusions and attacks on federal systems and systems supporting our nation's critical infrastructure, such as communications and financial services, have become more numerous, damaging, and disruptive. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. The National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015 require NCCIC to perform 11 cybersecurity-related functions, including sharing information and enabling real-time actions to address cybersecurity risks and incidents at federal and non-federal entities.

The two acts also contained provisions for GAO to report on NCCIC's implementation of its cybersecurity mission. For this report, GAO assessed the extent to which the NCCIC was performing the 11 required functions. To do this, GAO analyzed relevant program documentation, interviewed officials, and conducted a non-generalizable survey of 2,792 federal and nonfederal recipients of NCCIC products and services.

What GAO Recommends

GAO recommends nine actions to DHS for enhancing the effectiveness and efficiency of NCCIC, including to determine the applicability of the implementing principles and establish metrics and methods for evaluating performance; and address identified impediments. DHS concurred with GAO's recommendations.

View [GAO-17-163](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS) has taken steps to perform each of its 11 statutorily required cybersecurity functions, such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities. It manages several programs that provide data used in developing 43 products and services in support of the functions. The programs include monitoring network traffic entering and exiting federal agency networks and analyzing computer network vulnerabilities and threats. The products and services are provided to its customers in the private sector; federal, state, local, tribal, and territorial government entities; and other partner organizations. For example, NCCIC issues indicator bulletins, which can contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents and help to fulfill its function to coordinate the sharing of such information across the government.

The National Cybersecurity Protection Act also required NCCIC to carry out its functions in accordance with nine implementing principles, to the extent practicable. However, the extent to which NCCIC adhered to the 9 principles when performing the functions is unclear because the center has not yet determined the applicability of the principles to all 11 functions, or established metrics and methods by which to evaluate its performance against the principles. GAO identified instances where NCCIC had implemented its functions in accordance with one or more of the principles. For example, consistent with the principle that it seek and receive appropriate consideration from industry sector-specific, academic, and national laboratory expertise, NCCIC coordinated with contacts from industry, academia, and the national laboratories to develop and disseminate vulnerability alerts. On the other hand, GAO also identified instances where the cybersecurity functions were not performed in accordance with the principles. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities; however, it had not established measures or other procedures for ensuring the timeliness of these assessments. Until NCCIC determines the applicability of the principles to its functions and develops metrics and methods to evaluate its performance against the principles, the center cannot ensure that it is effectively meeting its statutory requirements.

In addition, GAO identified factors that impede NCCIC's ability to more efficiently perform several of its cybersecurity functions. For example, NCCIC officials were unable to completely track and consolidate cyber incidents reported to the center, thereby inhibiting its ability to coordinate the sharing of information across the government. Similarly, NCCIC may not have ready access to the current contact information for all owners and operators of the most critical cyber-dependent infrastructure assets. This lack could impede timely communication with them in the event of a cyber incident. Until NCCIC takes steps to overcome these impediments, it may not be able to efficiently perform its cybersecurity functions and assist federal and nonfederal entities in identifying cyber-based threats, mitigating vulnerabilities, and managing cyber risks.

Contents

Letter		1
	Background	3
	Although NCCIC Has Taken Steps to Perform Required Cybersecurity Functions, the Extent to Which It Carries Them Out In Accordance with Implementing Principles Is Unclear	15
	Conclusions	38
	Recommendations for Executive Action	39
	Agency Comments and Our Evaluation	39
Appendix I	Objective, Scope, and Methodology	41
Appendix II	NCCIC Product and Service Information	46
Appendix III	NCCIC Products and Services Supporting Cybersecurity Functions	50
Appendix IV	Examples of How NCCIC Products and Services Address the Implementing Principles	53
Appendix V	Comments from the Department of Homeland Security	56
Appendix VI	GAO Contact and Staff Acknowledgments	61
Tables		
	Table 1: National Cybersecurity and Communications Integration Center Statutorily Established Cybersecurity Functions	7
	Table 2: Nongeneralizable Survey Respondents' Use of Products and Services Provided by National Cybersecurity and Communications Integration Center's Components as a Percentage	34
	Table 3: Nongeneralizable Survey Respondents' Evaluation of the Effectiveness of National Cybersecurity and	

Communications Integration Center Activities as a Percentage	37
Table 4: Nongeneralizable Survey Respondents' Overall Evaluation of the National Cybersecurity and Communications Integration Center's Effectiveness in Carrying out of Its Mission as a Percentage	37
Table 5: Outcomes of GAO's National Cybersecurity and Communications Integration Center Customer Survey Sample	43
Table 6: Number of National Cybersecurity and Communications Integration Center (NCCIC) Products and Services Produced or Performed in Fiscal Years 2015 and 2016	46
Table 7: National Cybersecurity and Communications Integration Center Products and Services Used in Performing Prescribed Functions, as of October 2016	50
Table 8: Sample of Product and Services that Demonstrate How the National Cybersecurity and Communications Integration Center (NCCIC) Adhere to the Implementing Principles	53

Figures

Figure 1: NCCIC Organizational Chart	9
Figure 2: The National Cybersecurity and Communications Integration Center Watch Floor	10
Figure 3: National Cybersecurity and Communications Integration Center Reported Expenditures from Fiscal Year 2014 through Fiscal Year 2016	14
Figure 4: National Cybersecurity and Communications Integration Center's Preferred Methods to Receive Incidents	30

Abbreviations

CISCP	Cyber Information Sharing and Collaboration Program
CSET	Cyber Security Evaluation Tool
DHS	Department of Homeland Security
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISAC	Information Sharing and Analysis Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCC	National Coordinating Center
NCCIC	National Cybersecurity and Communications Integration Center
NO&I	NCCIC Operations and Integration
TLP	Traffic Light Protocol
US-CERT	U.S. Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



February 1, 2017

The Honorable Ron Johnson
Chairman
The Honorable Claire C. McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Michael McCaul
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Cyber-based intrusions and attacks on federal systems and systems supporting our nation's critical infrastructure, such as communications and financial services, have become not only more numerous and diverse but also more damaging and disruptive. This is illustrated by the data breach at the Office of Personnel Management, reported in July 2015, which impacted at least 21.5 million individuals and demonstrated the effect that such an incident can have on an agency's mission and national security. Protecting the information and control systems on which federal operations and national critical infrastructures depend and effectively responding to cyber incidents is critical because the unauthorized disclosure, alteration, and destruction of the information on those systems can result in great harm to those involved.

Since 1997, we have designated federal information security as a government-wide high-risk area and, in 2003, expanded this area to include computerized systems supporting the nation's critical infrastructure.¹ More recently, in the February 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information that is collected, maintained, and shared by both federal and nonfederal entities.

¹See GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: February 2015).

In 2009, the Department of Homeland Security (DHS) developed an integration center, the National Cybersecurity and Communications Integration Center (NCCIC), to provide a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats. The National Cybersecurity Protection Act of 2014 requires NCCIC to perform several cybersecurity functions, including being a federal civilian interface for sharing information on cybersecurity-related information and facilitating cross-sector coordination to address cybersecurity risks and incidents.² The act also required the center to adhere to nine principles, to the extent practicable, in carrying out these functions. One principle, for example, is ensuring that timely, actionable, and relevant information related to cybersecurity risks, incidents, and analysis is shared. The Cybersecurity Act of 2015 subsequently established additional functions for the center, among other things.³ These acts together identified 11 cybersecurity functions that the center is to perform.

In addition, the two acts included provisions for us to review NCCIC's efforts in carrying out its cybersecurity mission. For this review, our specific objective was to determine the extent to which NCCIC was performing its statutorily defined cybersecurity-related functions.

To do so, we reviewed the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015 to identify the center's statutorily defined functions and the principles for carrying out the functions. For each of the 11 functions identified in the acts, we analyzed relevant program documentation, including concepts of operations, program descriptions, analysis products, resource allocations, and performance measures. We also interviewed relevant NCCIC officials and analyzed the evidence provided to identify the products and services⁴ that the center develops and disseminates to federal and nonfederal entities and to learn how information sharing is coordinated and facilitated. We examined how these products and services are used in support of NCCIC's mandated

²Pub. L. No. 113-282, Dec. 18, 2014.

³The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

⁴NCCIC products are generally documents that can contain, among other things, information related to threats, malware or digital media analyses, or software vulnerabilities. Services can include activities to support the testing of emergency communications, incident response, or vulnerability assessments.

cybersecurity functions. In addition, we assessed the products and services against the nine principles outlined in the National Cybersecurity Protection Act of 2014 and interviewed relevant agency officials to determine how the center adhered to the principles.

Further, to supplement our work, we developed and administered a survey to a nongeneralizable sample of 2,792 recipients of the center's products and services to determine the effectiveness of current operations, products, and services in meeting their needs. The sample was randomly selected from a population of over 19,000 recipients maintained by NCCIC. The recipients included representatives from federal agencies and nonfederal entities, such as private-sector companies and organizations; state, local, tribal, and territorial governments; international partners; and individual citizens. We began our survey on August 2, 2016, and ended it on September 8, 2016.

The response rate to the survey, calculated as the number of usable responses⁵ received, divided by the number in the original sample found to be eligible⁶ was about 14 percent. Because of the low rate of response to the survey and other factors, the results can represent only illustrative responses from those responding, and are not generalizable to any larger population of recipients.

We conducted this performance audit from January 2016 to February 2017, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Additional details on our objective, scope, and methodology are contained in appendix I.

Background

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and

⁵An usable response refers to a survey questionnaire submitted with the sufficient amount of questions answered to be considered usable in our analysis.

⁶The eligible sample refers to the portion of the original sample remaining after removing ineligible sample members (e.g., undeliverable emails or responses from individuals who changed or otherwise left their position or employer).

electronic data to carry out operations and to process, maintain, and report essential information.⁷ Federal and nonfederal operations are largely supported by computer systems and electronic data, and organizations would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these cyber assets. Information security is, thus, especially important for federal and nonfederal entities to ensure the confidentiality, integrity, and availability of their systems and data.

Conversely, ineffective information security controls can result in significant risk to a broad array of operations and assets, as the following examples illustrate:

- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as personally identifiable information, intellectual property, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other crimes.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

The Nation Faces an Evolving Array of Cyber-Based Threats

Threats to systems are evolving and growing. Cyber threats can be unintentional or intentional. Unintentional or nonadversarial threat sources include failures in equipment or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters, as well as errors made by end users. They also include natural disasters and failures of critical infrastructure on which the organization depends, but that are outside of the control of the organization.

⁷Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. These critical infrastructures are: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

Intentional or adversarial threats include individuals, groups, entities, or nations that seek to leverage the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies). Threats can come from a wide array of sources, including corrupt employees, criminal groups, and terrorists. These threat adversaries vary in terms of their capabilities, their willingness to act, and their motives, which can include seeking monetary gain, or seeking an economic, political, or military advantage.

Cyber threat adversaries make use of various techniques, tactics, and practices, or exploits, to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. These exploits are carried out through various conduits, including websites, e-mails, wireless and cellular communications, Internet protocols, portable media, and social media. Further, adversaries can leverage computer software programs as a means by which to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program.

Reports of successfully executed cyber exploits illustrate the debilitating effects they can have on the nation's security and economy, and on public health and safety. Federal and nonfederal entities have experienced security breaches in their networks, potentially allowing sensitive information to be compromised, and systems, operations, and services to be disrupted. The examples that follow illustrate that a broad array of personal information and critical infrastructures are at risk:

- In October 2016, the International Atomic Energy Agency reported that a cyber attack had caused a disruption to the operations of a power plant. The agency did not disclose details about the information gathered or what specific operations were disrupted.
- In September 2016, Yahoo Incorporated, a multinational company,⁸ confirmed that 500 million user accounts were compromised. Yahoo company officials reported that the account information may have included names, e-mail addresses, telephone numbers, and dates of birth.

⁸Yahoo Incorporated, Yahoo! Help, accessed October 3, 2016, <https://help.yahoo.com/kb/sln27925.html>.

-
- In August 2015, the Internal Revenue Service reported that approximately 390,000 tax accounts were potentially affected by unauthorized third parties gaining access to taxpayer information from the agency's "Get Transcript" application. According to testimony from the Commissioner of Internal Revenue in June 2015, criminals had used taxpayer-specific data acquired from nonagency sources to gain unauthorized access to information, although at that time, the commissioner reported that approximately 100,000 tax accounts had been affected. The data included Social Security information, dates of birth, and street addresses.
 - In July 2015, the Office of Personnel Management reported that an intrusion into its systems had compromised the background investigation files of 21.5 million individuals. This was in addition to a separate but related incident that had affected the personnel records of about 4 million current and former federal employees, which the agency announced in June 2015.
 - In April 2015, the Department of Veterans Affairs' Office of Inspector General reported that two contractors had improperly accessed the agency's network from foreign countries using personally owned equipment.

Federal Law Established NCCIC as the Federal Civilian Center for Cybersecurity

In 2009, DHS developed NCCIC to provide a central place for federal and private-sector organizations to coordinate efforts to address cyber threats and respond to cyber attacks.⁹ The center's stated mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks.

The National Cybersecurity Protection Act of 2014 statutorily established the center's role within DHS to act as a federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings with federal and nonfederal entities, and to provide shared situational awareness to enable real-time actions to address cybersecurity risks and incidents to federal and nonfederal entities. The

⁹National Security Presidential Directive 54/Homeland Security Presidential Directive 23, establishing the Comprehensive National Cybersecurity Initiative, is aimed at safeguarding federal executive branch government information systems. The initiative directed DHS's establishment of NCCIC as well as the requirement for the center to coordinate with the various federal centers. White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

Cybersecurity Act of 2015 added roles for NCCIC and required DHS to create and issue several related policies and procedures.

Table 1 describes the 11 cybersecurity functions that NCCIC is to carry out, as prescribed by the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015.

Table 1: National Cybersecurity and Communications Integration Center Statutorily Established Cybersecurity Functions

Function	Description
1	Be a federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis and warnings for federal and nonfederal entities.
2	Provide shared situational awareness to enable real-time, integrated, and operational actions across the federal government and nonfederal entities to address cybersecurity risks and incidents to federal and nonfederal entities.
3	Coordinate the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents across the federal government.
4	Facilitate cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors.
5	Conduct and share integration and analysis, including cross-sector, of cyber threat indicators, defensive measures, cybersecurity risks and incidents with federal and nonfederal entities.
6	Provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks and incidents, which may include attribution, mitigation, and remediation.
7	Provide information and recommendations on security and resilience measures to federal and nonfederal entities, including information and recommendations to facilitate information security and strengthen information systems against cybersecurity risks and incidents; and share cyber threat indicators and defensive measures.
8	Engage with international partners, in consultation with other appropriate agencies, to (a) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and (b) enhance the security and resilience of global cybersecurity.
9	Share cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with federal and nonfederal entities, including across sectors of critical infrastructure and with state and major urban area fusion centers, as appropriate.
10	Participate, as appropriate, in national exercises run by the Department of Homeland Security (DHS).
11	Coordinate with the Office of Emergency Communications within DHS, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

Source: GAO analysis of National Cybersecurity Protection Act of 2014 and Cybersecurity Act of 2015. | GAO-17-163

Further, the National Cybersecurity Protection Act of 2014 states that the center shall ensure that it carries out these functions, to the extent practicable, in accordance with the following 9 principles:

1. Ensure that timely, actionable, and relevant information related to risks, incidents, and analysis is shared.

-
2. Ensure that when appropriate, information related to risks, incidents, and analysis is integrated with other information and tailored to a sector.
 3. Ensure that the activities are prioritized and conducted based on the level of risk.
 4. Ensure that industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration.
 5. Ensure that continuous, collaborative, and inclusive coordination occurs across sectors, with sector coordination councils, information sharing and analysis organizations, and other nonfederal partners.
 6. Ensure that, as appropriate, the center works to develop and use mechanisms for sharing information related to cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient.
 7. Ensure that the center works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents.
 8. Ensure that information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access.
 9. Ensure that activities conducted comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons.

Four Branches Within NCCIC Perform Cybersecurity-related Functions

To perform its functions, NCCIC is organized into four branches:

United States Computer Emergency Readiness Team (US-CERT) is responsible for leading efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the government and private sector.

Industrial Control Systems (ICS) Cyber Emergency Response Team (ICS-CERT) is responsible for taking steps to reduce risk to the nation's critical infrastructure by strengthening control systems¹⁰ security and resilience through public-private partnerships. In executing its mission,

¹⁰Control systems are computer-based systems that are used within many infrastructures and industries to monitor and control sensitive processes and physical functions.

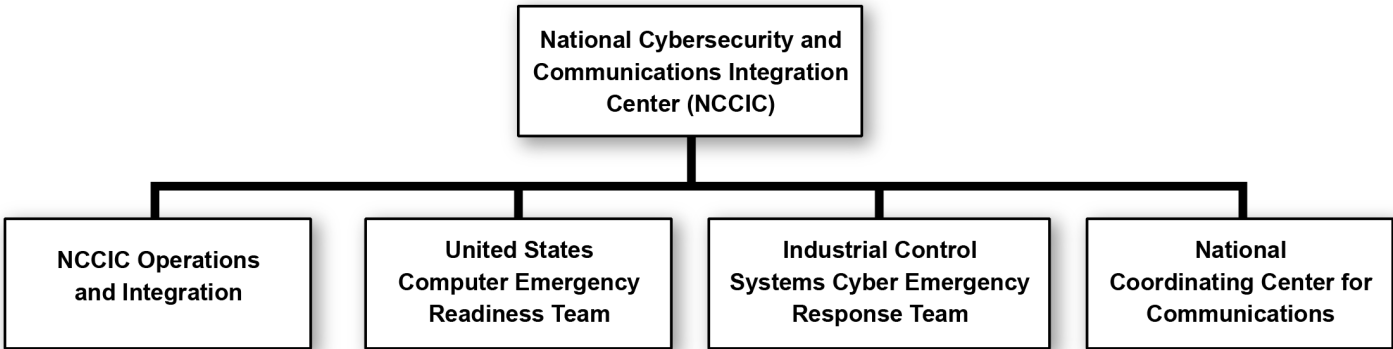
ICS-CERT is to serve its partners as the preeminent federal government resource for industrial control systems security.

National Coordinating Center for Communications (NCC) is responsible for helping government, private industry, and international partners to share and analyze threat information about, assess the operating status of, and understand the risk posture of the communications infrastructure. In addition, it is to coordinate efforts to prepare for, prevent, protect against, mitigate, respond to, and recover from significant communications disruptions.

NCCIC Operations & Integration (NO&I) is responsible for engaging in planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident response efforts across the center’s branches and activities.

Figure 1 shows the organizational structure of NCCIC.

Figure 1: NCCIC Organizational Chart



Source: Department of Homeland Security. | GAO-17-163

According to DHS policy, the cyber situational awareness, incident response, and management efforts of NCCIC’s four branches are to

occur on a 24-hour-a-day, 7-day-a-week basis at an integrated operations center known as the Watch Floor,¹¹ as shown in figure 2.

Figure 2: The National Cybersecurity and Communications Integration Center Watch Floor



Source: Department of Homeland Security, National Cybersecurity and Communications Integration Center. | GAO-17-163

NCCIC Works with Federal and Nonfederal Partners in Support of its Cybersecurity Mission

According to DHS policy, the center is to collaborate with federal departments and agencies most responsible for securing the government's cyber and communications systems. DHS policy and law also states that it is to engage with critical infrastructure¹² owners and operators; other private sector entities; state, local, tribal, and territorial

¹¹The NCCIC's Watch Floor is composed of integrated operations at one primary and two additional geographically dispersed locations. The primary Watch Floor provides a location for staff from each NCCIC component; members of other federal agencies; and representatives of nonfederal entities, including state governments and the private sector, to observe, work, and coordinate to maintain situational awareness of the cybersecurity related positions of federal and nonfederal entities, and coordinate incident response.

¹²The term "critical infrastructure," as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. §5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

Federal Organizations and Cybersecurity Centers

governments; and international partners. These federal and nonfederal entities, as well as individual citizens, represent NCCIC's customers that are recipients of its products, such as documents about threats, malware or digital media analyses, or software vulnerabilities; and services, which can include support for the testing of emergency communications, incident response, or vulnerability assessments.

According to DHS policy, NCCIC is to coordinate with its federal partners that focus on securing the federal information infrastructure, with the intent of integrating cyber center information to provide cross-domain situational awareness, analysis, and reporting on the composite state of U.S. cyber networks and communication infrastructure. In addition, the Comprehensive National Cybersecurity Initiative requires the center to foster partnerships with other key federal cybersecurity and communications centers in order to collaborate and improve cybersecurity and communications infrastructure across the federal government.¹³ The federal centers include:

- Defense Cyber Crime Center sets standards for digital evidence processing, analysis, and diagnostics for Department of Defense investigations that require computer forensic support to detect, enhance, or recover digital media, including audio and video.
- Intelligence Community Security Coordination Center provides attack sensing and warning capabilities to characterize cyber threats and attributions of attacks, and anticipates future incidents.
- National Cyber Investigative Joint Task Force, organized by the Federal Bureau of Investigation, serves as a focal point for all government agencies to coordinate, integrate, and share information related to domestic cyber threat investigations.
- National Security Agency/Central Security Service Threat Operations Center establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity.
- United States Cyber Command Joint Operations Center establishes and maintains situational awareness and directs the operations and defense of the ".mil" networks.

¹³The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23. (Washington, D.C.: Jan. 8, 2008).

Private Sector and Critical Infrastructure Owners and Operators

- National Infrastructure Coordinating Center is the coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government.

DHS policy also states that each of these federal cybersecurity and communications centers is to provide complementary capabilities and resources that collectively form the threat characterization, vulnerability analysis, information sharing, detection and response, investigation, and defense of civilian federal cyber networks and communication infrastructures.

NCCIC works with the private sector that owns and operates most of the nation's critical infrastructure, such as banking and financial institutions, telecommunications networks, and energy production and transmission facilities. Infrastructure owners and operators are to integrate (both physically and virtually) into the center's operations so that, during an incident, information can be aggregated and communicated between government and appropriate private sector partners in an efficient manner. As of August 2016, 174 private sector companies had as-needed access to NCCIC through their participation in the Cyber Information Sharing and Collaboration Program (CISCP).¹⁴

As part of this effort, NCCIC is to coordinate on an ongoing basis with various private sector partners, including information sharing and analysis centers (ISAC)¹⁵ and technology vendors. ISACs have been formed for a number of sectors. According to the National Council of ISACs, these include (1) automotive; (2) aviation; (3) defense industrial base; (4) emergency services; (5) electricity; (6) financial services; (7) healthcare; (8) information technology; (9) maritime security; (10) communications; (11) multistate; (12) national health; (13) oil and gas; (14) public transit; (15) real estate; (16) retail; (17) research and education; (18) supply

¹⁴The goal of CISCP is to provide a bilateral exchange of cyber threat indicators. The program is to provide a platform and a trusted forum for exchanging threat and vulnerability information, governed by a Cooperative Research and Development Agreement (CRADA) between DHS and each CISCP participant. The CRADA allows participants to gain as-needed access to NCCIC, a mechanism to receive security clearances, and the ability to participate in bi-directional information sharing.

¹⁵Information Sharing and Analysis Centers are to help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. They typically collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

chain; (19) surface transportation; and (20) water.¹⁶ As of October 2016, five nonfederal entities maintained a permanent presence on the NCCIC Watch Floor (the ISACs of the financial, national health, aviation, and energy sectors, as well as the Multi-State ISAC).

State, Local, Tribal, and Territorial Governments

NCCIC maintains partnerships with state, local, tribal, and territorial governments to support their protection of each respective community. These governments are responsible for the security and integrity of their own cyber networks, along with associated preparedness, mitigation, and response efforts.

The center is to facilitate overarching situational awareness and the sharing of technical information and best practices with these nonfederal government partners to help ensure a strengthened national cyber risk posture. As part of this effort, NCCIC is to coordinate on an ongoing basis with the Multi-State Information Sharing and Analysis Center (MS-ISAC), and an MS-ISAC representative is physically located on the NCCIC Watch Floor.

International Partners

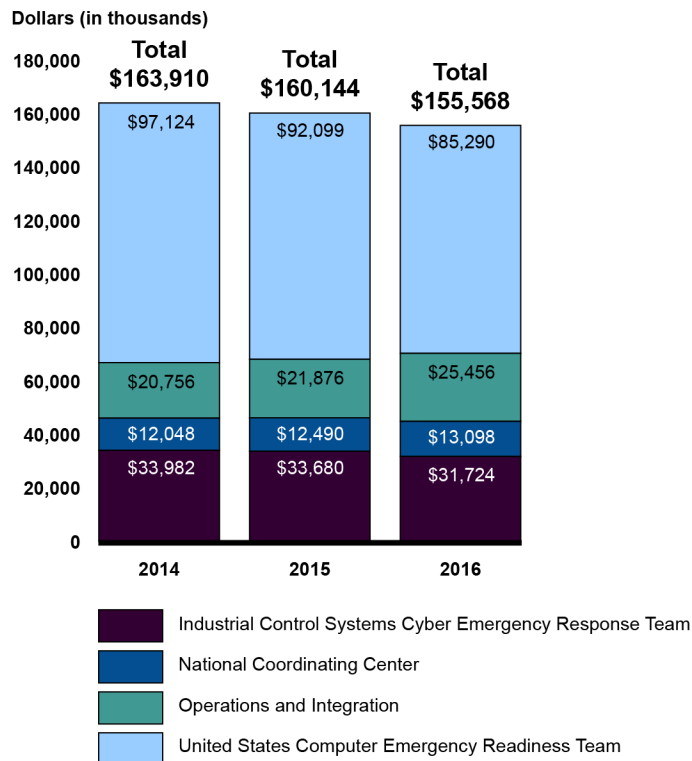
As part of its mission, NCCIC also engages and collaborates with international partners, including governments that are members of the North Atlantic Treaty Organization (NATO), to disseminate bulletins and perform services. The center works with international partners and their respective cyber centers while conducting cyber-related exercises —as part of a March 2016 exercise, representatives from Australia, Canada, Denmark, Finland, Germany, Hungary, Japan, Netherlands, New Zealand, Sweden, Switzerland, and the United Kingdom participated. NCCIC also can assist international partners with responding to cyber incidents. For example, during the cyber attack against the Ukrainian power infrastructure in December 2015, the center collaborated with the Ukrainian government to determine the methods of the cyber attack.

¹⁶The National Council of ISACs functions as a cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. See <http://www.nationalisacs.org/>

NCCIC Reported Spending about \$480 Million over the Past Three Fiscal Years

NCCIC reported that it spent about \$480 million on cybersecurity-related activities during fiscal years 2014 through 2016. According to the center's officials, this included spending for 262, 268, and 301 full-time employees for each of the three fiscal years, respectively. Figure 3 depicts the reported expenditures per year by each of the four branches of NCCIC.

Figure 3: National Cybersecurity and Communications Integration Center Reported Expenditures from Fiscal Year 2014 through Fiscal Year 2016



Source: GAO analysis of Department of Homeland Security information. | GAO-17-163

Although NCCIC Has Taken Steps to Perform Required Cybersecurity Functions, the Extent to Which It Carries Them Out in Accordance with Implementing Principles Is Unclear

NCCIC has taken steps to perform each of its 11 statutorily required cybersecurity functions. It has developed a variety of products and services in support of these functions, including those related to analyzing and sharing cyber information, facilitating coordination among federal and nonfederal partners, and conducting technical assistance and exercises. However, the extent to which NCCIC carried out these functions in accordance with the nine principles specified in the National Cybersecurity Protection Act of 2014 is unclear because the center has not consistently evaluated its performance against the principles. In addition, a number of factors impede NCCIC's ability to more efficiently perform several of its cybersecurity functions. Although not generalizable to any larger population, recipients of its products and services that responded to our survey expressed generally favorable views of its activities. Nevertheless, NCCIC has limited assurance that it is fully meeting statutory requirements and efficiently performing its cybersecurity functions because it has not completely evaluated its performance against the principles or addressed the impediments to performing its cybersecurity functions.

NCCIC Has Developed a Variety of Products and Services in Support of Required Cybersecurity Functions

NCCIC has developed 43 types of products and services in support of its 11 statutorily required functions. Descriptions of these products and services as well as the total numbers of each provided to NCCIC's customers during fiscal years 2015 and 2016 are discussed in greater detail in appendix II. The center manages several programs that provide data used in developing the products and performing the services related to its cybersecurity functions. These programs include:

- The National Cybersecurity Protection System, operationally known as EINSTEIN, monitors network traffic entering or exiting networks of federal agencies and provides intrusion detection and intrusion prevention services. NCCIC analysts use data logged by EINSTEIN to

notify federal and nonfederal partners of potential breaches of information security.¹⁷

- The Advanced Malware Analysis Center is a set of capabilities intended to provide a segregated, closed, computer network system that is used to analyze computer network vulnerabilities and threats. According to NCCIC officials, information transmitted to NCCIC through the Advanced Malware Analysis Center may include malicious codes, computer viruses, worms, spyware, bots, and Trojan horses. Once received, analysts use the malware analysis capabilities to analyze the code or images in order to discover how to secure or defend computer systems against the threat. The corrective action information is then published in products such as vulnerability reports or alerts or malware reports.
- The Automated Indicator Sharing program was created to provide real-time sharing of cyber threat indicators and defensive measures by enabling NCCIC to (1) receive cyber threat indicators and defensive measures submitted by its nonfederal participants and federal entities; (2) remove personally identifiable information and other sensitive information that is not directly related to a cybersecurity threat; and (3) disseminate the cyber threat indicators and defensive measures to its nonfederal participants and federal entities, as appropriate. The Automated Indicator Sharing program uses the DHS-developed Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information formats, a mechanism for sharing cyber threat information in a common manner.¹⁸ NCCIC uses this program to send out machine-readable cyber threat indicators at near-real-time and is now onboarding participants across the public and private sectors. NCCIC

¹⁷In January 2016, we reported that DHS's National Cybersecurity Protection System had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information. In addition, adoption of these capabilities at federal agencies was limited. We recommended that the Department of Homeland Security expand the system's capabilities for detecting and preventing malicious traffic, define requirements for future capabilities, and develop network routing guidance to increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies. DHS generally agreed with our recommendations and indicated it would act on them. For more details, please review GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, [GAO-16-294](#), (Washington, D.C.: Jan. 2016).

¹⁸DHS program documentation stated these formats allow public and private sector partners to share cyber threat information in the same way so that computers can immediately use the information for network defense.

officials stated that the Automated Indicator Sharing program was first disseminated to the 5 cyber centers. Since then, the program has become accessible to additional entities. According to the officials, as of August 2016, 32 private sector entities representing 6 critical infrastructure sectors and 7 federal agencies were connected to the program. NCCIC officials stated that DHS is in the process of expanding the service to all 24 Chief Financial Officers Act agencies in response to guidance from the Office of Management and Budget from October 2015.¹⁹

The following summarizes NCCIC's products and services²⁰ that support its 11 statutorily required functions. Details on how all 43 products and services support each of the cybersecurity functions are in appendix III.

Function 1: Be a federal civilian interface for the multidirectional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis and warnings for federal and nonfederal entities.

NCCIC has nine products and services that support this function. Among these, it provides products such as Cyber Information Sharing and Collaboration Program (CISCP) Indicator Bulletins²¹ and US-CERT Indicator Bulletins,²² which can include cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings. For fiscal year 2016, the center developed and disseminated 151 US-CERT Bulletins. For example, one US-CERT Bulletin identified Internet protocol

¹⁹There are 24 agencies identified in the Chief Financial Officers Act: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

²⁰NCCIC's customers are recipients of NCCIC products and services and include critical infrastructure owners and operators; other private sector entities; state, local, tribal, and territorial governments; and international partners; as well as individual citizens.

²¹CISCP Bulletins provide incident analysis information derived from new cyber incidents and/or malicious code, threats, and vulnerabilities to CISCP partners including local and state government, Critical Infrastructure (CI), private industry, or a country CERT.

²²US-CERT Indicator Bulletins are short turnaround bulletins containing threat-specific indicators of compromise.

addresses that had conducted unauthorized scans of networks of partner entities.

NCCIC also provides services to interface with federal and nonfederal entities. Through the center's Information Sharing and Liaison Services,²³ representatives from federal and nonfederal sectors are able to reside permanently or temporarily on the Watch Floor alongside NCCIC officials, to better ensure multidirectional, cross-sector sharing of information. According to the officials, there are seven seats available on the Watch Floor that its partners can reserve as a temporary residence. As of August 2016, the center reported agreements with 118 entities that could elect to reside temporarily on the Watch Floor. We observed additional cross-sector information sharing through the presence on the NCCIC Watch Floor of liaison officers from the other five cyber centers; members from the Multi-State, Communications, and Financial Services ISACs; and the intelligence community working in conjunction with NCCIC analysts.

Function 2: Provide shared situational awareness to enable real-time, integrated, and operational actions across the federal government and nonfederal entities to address cybersecurity risks and incidents to federal and nonfederal entities.

NCCIC supports this function with the use of 12 products and services. Among these products, it provides situational awareness to its customers to enable real-time, integrated, operational actions. Through one such product, Watch Floor Situation Reports,²⁴ the center provides awareness of incidents and recommendations on remediation. For example, one report disseminated to its partners identified current events related to Ransomware incidents directed towards hospitals. As part of the report, the center identified immediate and future actions in support of resolving the incidents. In addition, in providing notifications, such as National Coordinating Center for Communications (NCC) Watch Train

²³Information Sharing and Liaison Services, is a service whereby the center provides dedicated seats on the NCCIC Watch Floor for representatives of federal and nonfederal entities.

²⁴These reports are delivered after an incident has occurred based on what NCCIC knows and does not know regarding the incident. Reports are tailored for specific sectors and may be updated when further analysis has been conducted by NCCIC.

Derailment²⁵ and GPS Testing Notices,²⁶ the center shared information to support operational actions on behalf of the partner entities. Further, NCCIC provided situational awareness of potentially malicious Internet protocol addresses through Victim/Abuse notifications.²⁷

Function 3: Coordinate the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents across the federal government.

NCCIC has nine products and services that support this function. Among the products are CISCP Bulletins, US-CERT Bulletins, Joint Analysis Reports,²⁸ and Joint Indicator Bulletins²⁹ that can contain information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents. For example, the center issued eight Joint Analysis Reports during fiscal years 2015 and 2016. One report, issued jointly with the Federal Bureau of Investigation on April 14, 2015, was also coordinated with the Departments of Treasury and Energy. The report contained a summation of open-source analysis related to common vulnerabilities leveraged by state-sponsored cyber operators in products such as Adobe Flash, Adobe Reader, Microsoft Office, Microsoft server software, and OpenSSL. The report contained information on the specific version of the product affected, as well as the associated information to patch the vulnerability.

According to NCCIC officials, the center relies on the NCCIC Portal³⁰ as a mechanism to coordinate the sharing of these products to customers.

²⁵Notification of communications disruption is disseminated to government and industry partners, as a result of an incident identification from the Department of Transportation Crisis Management Center.

²⁶Notification of a scheduled test in a geographical area is made to determine if there are equipment malfunctions or external problems (e.g., natural disaster) with a communications medium.

²⁷A victim notification is sent to a third party based on information that they may be a victim of a cybersecurity event. An abuse notification is sent to a third party based on information that they may have systems that are being used for malicious purposes.

²⁸An analysis report is produced in coordination with US-CERT's trusted partners (i.e., law enforcement or intelligence community).

²⁹An indicator bulletin is produced in coordination with US-CERT's trusted partners (i.e., law enforcement or intelligence community).

³⁰The NCCIC Portal was formerly known as the US-CERT Portal.

Specifically, the portal is comprised of 35 compartments, which include customers across the globe, and within government and various critical infrastructures. Each of the compartments represents a grouping of entities with a similar role or focus. For example, the Government Forum of Incident Response and Security Teams are comprised of individuals from federal civilian and military agencies responsible for securing government information technology systems.

Function 4: Facilitate cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts, across multiple sectors.

NCCIC has six products and services that support this function. For example, the center facilitates cross-sector coordination to address cybersecurity risks and incidents through its Industrial Control Systems Joint Working Group³¹ and its Incident Notifications.³² In particular, the joint working group holds biannual meetings with the industrial control system community. For example, the most recent meeting occurred on May 3–5, 2016, and had over 300 stakeholders represented. According to the after-action report, representatives from several sectors, including officials from the energy, water, transportation, and nuclear sectors, among others, attended the meeting.

Function 5: Conduct and share integration and analysis, including cross-sector, of cyber threat indicators, defensive measures, cybersecurity risks and incidents with federal and nonfederal entities.

NCCIC has eight products and services that support this function. For example, the US-CERT Analysis Report³³ is an integrated analysis document that can contain indicators of compromise and tactics, techniques, and procedures related to specific threats. Further, US-CERT officials stated that the center provides common vulnerabilities to the

³¹The working group is a collaborative and coordinating body that provides a vehicle for communicating and partnering across all Critical Infrastructure Sectors between federal agencies and departments, as well as private-asset owners/operators of industrial control systems.

³²US-CERT detects malicious cyber activity targeting federal agencies through tools such as EINSTEIN.

³³Provides indicators of compromise and tactics, techniques, and procedures related to specific threats.

National Vulnerability Database,³⁴ which is an established, open source of indicators used by information security professionals located across the nation and throughout the world. Further, ICS-CERT officials stated that it provides industrial control system vulnerabilities to over 15,000 “.gov” e-mail addresses that are signed up to receive ICS-CERT Vulnerability Alerts.³⁵

Function 6: Provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities with respect to cyber threat indicators, defensive measures, and cybersecurity risks and incidents, which may include attribution, mitigation, and remediation.

NCCIC supports this function with the use of five products and services. With these products, it has the capacity to provide technical assistance, risk management support, and incident response capabilities to customers upon request. For example, in responding to and conducting incident response analyses for public or private sector customers, US-CERT developed Incident Response Team Reports that outlined mitigation recommendations to the customers.

In addition, to support risk management, the center conducted, as services, Risk and Vulnerability Assessments, which are activities to assist entities in developing strategies for improving their cybersecurity posture. According to officials, NCCIC attempts to provide a report of its findings to the requesting entity within 30 days of the assessment.

Further, NCCIC provided Cyber Assessments³⁶ of control systems. For example, the Cyber Security Evaluation Tool (CSET®) can be downloaded to conduct a self-evaluation of an entity’s cybersecurity posture against, among other things, best practices and National Institute

³⁴The database provides information about software vulnerabilities, including summaries, technical details, remediation information, and lists of affected vendors. Many vulnerability notes are the result of private coordination and disclosure efforts.

³⁵An alert from ICS-CERT indicates an identified vulnerability and spells out what actions an entity can take to mitigate the vulnerability, including implementing a patch.

³⁶Assessments include a Design Architecture Review, a technical review and cyber evaluation of industrial control system operations; a CSET, a basic one day assessment ending in a report on the organization’s cyber posture; and a Network Architecture Verification and Validation, where DHS uses tools to review and analyze network traffic occurring within the industrial control system network.

of Standards and Technology recommendations. In addition, ICS-CERT officials stated that upon a customer's request, NCCIC can provide further assistance by conducting industrial control system architectural assessments and network assessments.

Function 7: Provide information and recommendations on security and resilience measures to federal and nonfederal entities, including information and recommendations to facilitate information security and strengthen information systems against cybersecurity risks and incidents; and share cyber threat indicators and defensive measures.

NCCIC has 16 products and services that support this function. Among these products, the center provided information and recommendations on security and resilience measures through its Preliminary Digital Media Analysis Report³⁷ and Digital Media Analysis Report³⁸ products. Specifically, for these products, it conducted analysis of digital media and provided a report that includes analysis of the exploits and associated mitigation strategies. Further, according to NCCIC officials, the US-CERT and ICS-CERT components conduct incident response activities (known as US-CERT Incident Response Team Report³⁹ and ICS Incident Response Deployment⁴⁰) and develop reports to document their findings at the request of partner entities. These reports can contain recommendations to strengthen information systems against cybersecurity risks and incidents and potentially share cyber threat indicators and defensive measures.

Function 8: Engage with international partners, in consultation with other appropriate agencies, to (a) collaborate on cyber threat indicators,

³⁷These are reports of initial findings from a forensic investigation of digital media.

³⁸These are reports of full forensic analysis of digital media.

³⁹This is a report provided to external customers on the impact of a particular compromise. For example, officials stated that their activities to assist the Office of Personnel Management during its information breach would fall under this product. An output of this product would be a report to the affected party. Other outputs of this product may result in binding operational directives to agencies, or information for OMB memoranda. The Federal Information Security Modernization Act of 2014 gives statutory authority to DHS to issue binding operational directives to federal agencies regarding the specific actions that agencies need to take to address specific cyber threats and vulnerabilities. Implementation of these directives is compulsory for the agencies.

⁴⁰Incident-response assistance is provided either on-site or remotely and incident analysis is provided that varies based upon the nature of the cybersecurity incident.

defensive measures, and information related to cybersecurity risks and incidents; and (b) enhance the security and resilience of global cybersecurity.

NCCIC supports this function with the use of 10 products and services. It engages with international partners to collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents. For example, the most recent Cyberstorm exercise—the department’s national-level exercise⁴¹ series—was conducted during the spring of 2016 and involved more than 1,200 participants including NCCIC’s national and international partners. According to the exercise after-action report, 12 international partners participated in the Cyberstorm exercise. To enhance the security and reliance of global cybersecurity, the after-action report identified areas of improvement relating to the escalation of incidents and coordination of public and private efforts. ICS-CERT also collaborated with the Ukrainian government in the aftermath of a cyber attack on its power infrastructure to develop and disseminate vulnerability alerts, reports, and briefings on the attack. US-CERT, on a different occasion, collaborated with Canada on developing vulnerability alerts associated with ransomware.

Function 9: Share cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with federal and nonfederal entities, including across sectors of critical infrastructure and with state and major urban area fusion centers,⁴² as appropriate.

NCCIC relies on four products and services to support this function. For example, it shared cyber threat indicators, defensive measures, and information through its Malware Initial Findings Reports⁴³ and Malware Analysis Reports.⁴⁴ These reports are based on NCCIC malware analysis conducted at the request of the customer. They can contain indicators,

⁴¹These exercises are longer and orders of magnitude more costly than a regular exercise and can involve thousands of participants. Examples include Cyberstorm and Cyberguard.

⁴²Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information among federal; state, local, tribal, territorial (SLTT); and private sector partners.

⁴³The reports provide preliminary analysis and initial mitigation recommendations for submitted malware artifacts.

⁴⁴These reports contain full analysis, indicators of compromise, tactics, techniques, and procedures, and mitigation recommendations for submitted malware artifacts.

such as a description of the malware artifact, as well as defensive measures, such as the Internet Protocol addresses potentially associated with the malware.

Both types of reports are disseminated via the NCCIC Portal. The center used a Traffic Light Protocol (TLP), which is a designation to ensure that sensitive information is shared with the appropriate audience.⁴⁵ MS-ISAC representatives have access to the NCCIC portal and can share information with its members per TLP protections.

Function 10: Participate, as appropriate, in national exercises run by the department.

NCCIC has four products and services that support this function. For example, in addition to Cyberstorm, the center conducted and participated in external exercises for customers to support the improvement of national and international cybersecurity. NCCIC officials stated that these external exercises⁴⁶ include federal, state, local, tribal, territorial, private, and international partners and range from individual table-top exercises to multi-organization exercises. The center conducted such an exercise in October 2015 with a state government to improve its communication capabilities and provided a seminar on the current threats to control systems worldwide.

Function 11: Coordinate with the Office of Emergency Communication of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

⁴⁵Traffic Light Protocol (TLP) has four colors (red, amber, green, and white) that it uses to designate the sharing limitations of information. For example, for TLP: Red, recipients may not share information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. For TLP: Amber, recipients may only share information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. For TLP: Green, recipients may share information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: White may be shared without restriction.

⁴⁶Other examples are when NCCIC is asked to teach an entity how to conduct exercises, manage a cyber exercise or provide analysis on an exercise already completed.

NCCIC has four products and services that support this function. Among its activities, the center engages with the Office of Emergency Communications in planning and preparing for disasters and incidents, including cyber incidents, to ensure continued readiness of the communications network. NCCIC officials stated they meet weekly with Office of Emergency Communications Regional coordinators during a NCC Weekly Operations call to discuss threats and vulnerabilities. According to NCCIC, the Office of Emergency Communications is a supporting partner of its execution of national coordinator responsibilities for Emergency Support Function 2–Communications under the National Response Framework.⁴⁷ In addition, officials from the center have briefed the National Council of Statewide Interoperability Coordinators on how to share cyber data using NCCIC’s incident reporting process at a national conference in April 2016.

NCCIC’s Adherence to the Implementing Principles in Carrying Out its Cybersecurity Functions Is Unclear

NCCIC is required to carry out its functions in accordance with nine principles specified in the National Cybersecurity Protection Act of 2014, to the extent practicable. As previously described, these principles, among other things, relate to ensuring that industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration; the information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access; and shared information is timely, actionable, and relevant to risks, incidents, and analysis.

The extent to which NCCIC carried out its 11 cybersecurity functions in accordance with the nine principles specified in the act is unclear. We identified instances where, with certain products and services, NCCIC had implemented its functions in adherence with one or more of the principles. For example, consistent with the principle that it seek and receive appropriate consideration from industry sector-specific, academic, and national laboratory expertise, NCCIC coordinated with contacts from industry, academia, and the national laboratories to develop and disseminate vulnerability alerts through the National Vulnerability Database.⁴⁸ In addition, to comply with the principle that the information

⁴⁷The Emergency Support Function 2 is to provide communications support to federal, state, tribal, and local governments and first responders when their systems have been impacted in non-wartime emergencies.

⁴⁸Vulnerability alerts support functions 5, 7, and 8.

related to cybersecurity risks and incidents be appropriately safeguarded against unauthorized access, the center used the TLP designation to ensure that sensitive information was shared with the appropriate audience. Specifically, NCCIC disseminated its products via the NCCIC portal, using the protocol for products such as Indicator Bulletins, Analysis Reports, Malware Initial Findings Reports, and Malware Analysis Reports.⁴⁹ (Additional examples of how NCCIC products and services helped the center implement its functions according to the principles are provided in appendix IV.)

On the other hand, we also identified instances where the cybersecurity functions were not performed in adherence with the principles. For example, with regard to function 6, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities. The function is supported, in part, by Risk and Vulnerability Assessments. However, NCCIC had not established measures or other procedures for ensuring the timeliness of these assessments. According to officials responsible for this service, the assessments have an estimated completion time frame of 8-10 weeks for each customer. However, the officials stated that this time frame is not an established metric by which they evaluate the timeliness of the service. Further, NCCIC had not established measures or procedures to assess the actionability of its products and services. For example, US-CERT Indicator Bulletins, a product that supports several functions,⁵⁰ typically contain actionable information, such as specific malicious Internet addresses to be blocked. NCCIC had not established a means of determining the extent to which a particular bulletin helped to mitigate a risk or prevent an incident.

In discussing this matter, NCCIC officials acknowledged that they had not made a complete determination of the applicability of the principles with all of the center's functions and thus had not established measures and procedures for assessing its products and services against the principles. The officials stated that they have begun to map activities supporting the cybersecurity functions to the implementing principles. For example, according to the officials, the center established a unit for reviewing and

⁴⁹Indicator Bulletins support functions 1, 2, 3, and 5; Analysis Reports support functions 2 and 5; Malware Initial Findings Reports support function 8 and 9; and Malware Analysis Reports support function 9.

⁵⁰US-CERT Indicator Bulletins support functions 1, 2, 3, and 5.

making recommendations to improve overall NCCIC operations. During fiscal year 2016, this unit completed performance management reviews⁵¹ across the center's programs to identify areas in which NCCIC could better align its operations with its overall requirements, including the principles. Further, officials from the ICS-CERT branch stated that they were in the preliminary stages of measuring their activities against one of the nine principles. Specifically, the officials stated that 20 metrics were being developed⁵² that would measure timeliness, relevance, and actionability (principle 1) across the components of their organization.

Nevertheless, while these preliminary actions are important steps, they do not represent a complete determination of the applicability of all nine principles across all of NCCIC's statutorily-required cybersecurity functions. As such, NCCIC officials could not say whether the principles did or did not apply to all of the 11 functions. Moreover, because a complete determination of the applicability of the nine principles had not been done, the center also had not developed metrics and methods for assessing and ensuring adherence with the principles. Until the center determines the applicability of the implementing principles for all of its functions and develops the metrics and methods necessary to ensure that the principles are met, it will not be positioned to ensure that NCCIC is effectively meeting its statutory requirements.

NCCIC Faces Impediments to Performing Its Cybersecurity Functions More Efficiently

In addition to NCCIC not having made a complete determination of how it is adhering to the principles, a number of factors impede the center's ability to more efficiently perform several of its cybersecurity functions. In particular, the center faces impediments in tracking security incidents; maintaining current and reliable customer information, to include obtaining such information on all owners and operators of the most critical infrastructure assets; working across multiple network platforms; and collaborating with international partners.

⁵¹The Center conducts these reviews center-wide for each program, at 6-month intervals. The reviews conducted to date were performed to identify program-specific measures, success stories, customer feedback, personnel resources, and areas for improvement. The reviews identified areas needing improvement, such as inefficiencies in developing and disseminating products and services, and related recommendations.

⁵²We were unable to evaluate the metrics developed by ICS-CERT as they were in the preliminary stages of development.

Tracking of security incidents is not centralized or reconciled. The National Cybersecurity Protection Act of 2014 requires NCCIC to coordinate the sharing of information across the government. This includes information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents.

However, NCCIC officials were unable to completely track and consolidate cyber incidents⁵³ reported to the center, thereby inhibiting its ability to coordinate the sharing of information across the government. For US-CERT-related incidents, personnel assigned to the NCICC service desk generated a daily report of the current status of the open incident tickets. For example, the July 18, 2016 report had a total of 520 incident tickets. However, this report did not represent the totality of incidents across the center because it did not include incidents reported to ICS-CERT. Since the NCCIC service desk did not have access to the data within the ICS-CERT ticketing system, it could not produce a management report on the status of all incidents reported to the center.

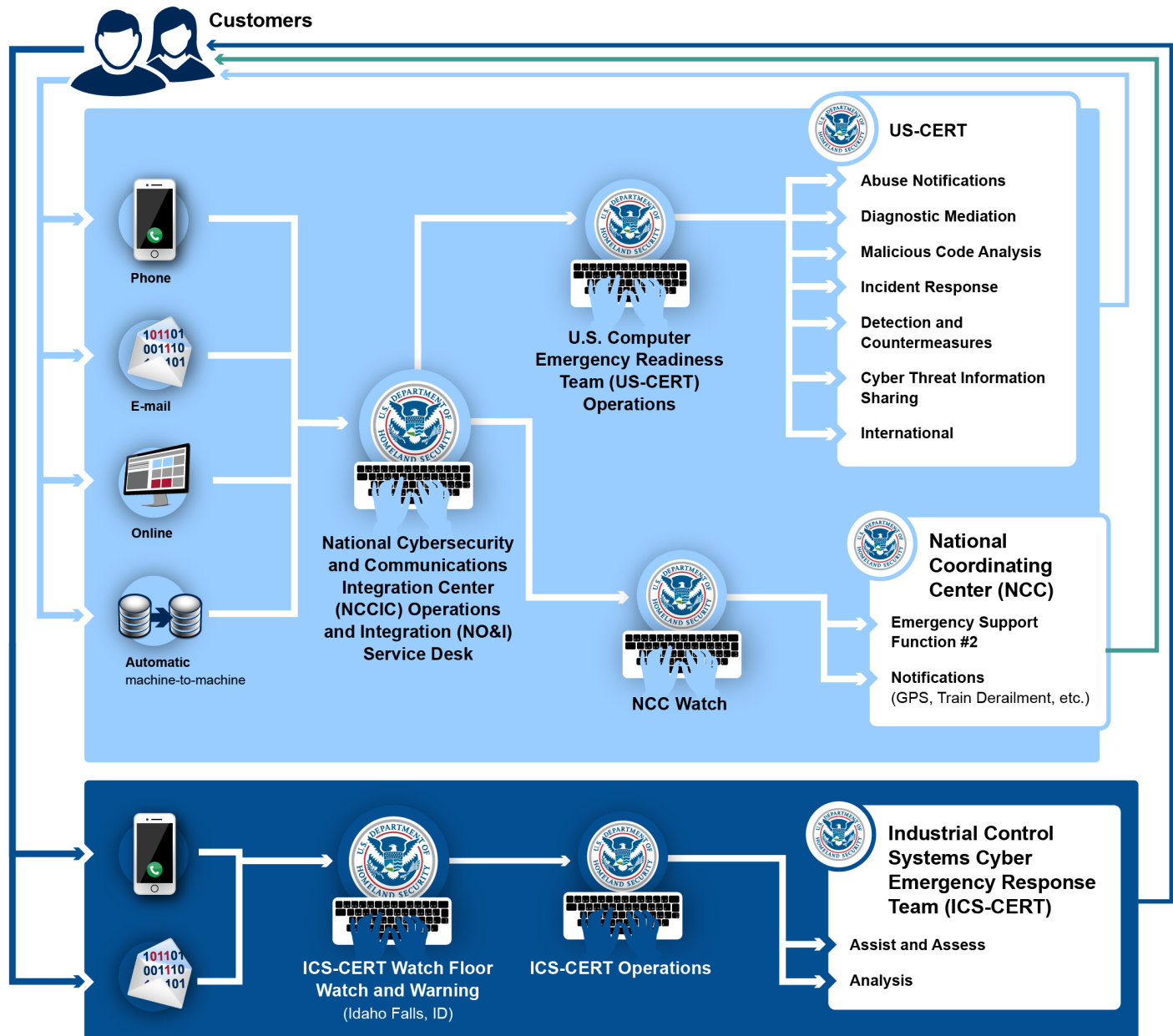
NCCIC officials attributed the lack of a single, centralized incident tracking system to the fact that ICS-CERT and US-CERT had operated as separate entities prior to the establishment of the center. As such, both ICS-CERT and US-CERT has its own incident ticketing system. Senior ICS-CERT officials stated they are aware of this challenge and are exploring options on how best to integrate the two systems. Until such integration takes place, NCCIC will continue to encounter difficulty in completely tracking the total efforts of its branches to address reported cybersecurity incidents. As a result, the center will be challenged in determining how effective it is in sharing information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents across the government.

The difficulty of logging incident data is further compounded by the multiple ways in which an incident can be reported to the center. US-CERT officials stated that there are six preferred ways in which NCCIC receives information related to potential incidents. For example, to communicate with US-CERT, customers can choose e-mail, a phone call,

⁵³ A cyber incident is a security breach of a computerized system. The National Institute of Standards and Technology defines an incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. The terms information security and information security incident apply more broadly to any forms of information and systems.

an automatic submission form, or an automated machine-to-machine submission as the means to notify US-CERT of an incident. In addition, to communicate with ICS-CERT regarding an industrial control system-related incident, customers can choose to submit an e-mail or phone directly to ICS-CERT (Figure 4 shows the ways in which NCCIC prefers to receive reported incidents.)

Figure 4: National Cybersecurity and Communications Integration Center's Preferred Methods to Receive Incidents



Source: GAO analysis based on Department of Homeland Security information. | GAO-17-163

However, contrary to the 6 preferred methods of communicating with US-CERT and ICS-CERT, officials from NCCIC's Operations and Integration office provided documentation that identified at least 22 methods by which the center receives potential incidents. These methods would include phone numbers and e-mail addresses other than the aforementioned 6 methods, established by various groups within the four NCCIC components as a means to communicate with partners.

In addition, according to NCCIC officials, depending on the method of reporting, incidents are not always logged into the NCCIC incident ticketing systems. For example, when customers have prior established relationships, analysts can be called directly and can handle the incidents without logging them into the system. The lack of control over the entry points as well as inconsistencies in logging data, together, inhibit the center in consistently tracking incidents and their status across the entire NCCIC.

Until the center can reduce, consolidate, or modify the points of entry that customer entities use to communicate with NCCIC, it will lack the ability to better ensure that all incident tickets are logged appropriately. Thus, further contributing to the center being less able to effectively perform its statutorily-required function in coordinating the sharing of information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents across the government.

Maintaining current and reliable customer information. The National Cybersecurity Protection Act of 2014 requires NCCIC to be the federal civilian interface for the multidirectional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents, and analysis and warnings for federal and nonfederal entities. To perform this function, the center needs to have accurate and up-to-date contact information for the potential recipients of the cybersecurity information it shares.

However, NCCIC's contact information was not always up to date, thus impacting its ability to effectively function as a federal civilian interface for federal and nonfederal entities. Specifically, after e-mailing our survey to recipients of NCCIC's products and services, we received 303 undeliverable return messages out of 2,792 recipients contacted. We also identified individuals who were included on the list of recipients that NCCIC provided to us that no longer had the role the center indicated or were no longer with the entity listed.

NCCIC officials were unable to demonstrate that they had any formal process for maintaining customer contact information. The officials stated that maintaining customer contact information was an ad hoc process and acknowledged that capturing changes to that data was a challenge.

Without regularly validating data pertaining to its product and service recipients, the center may lack quality information it needs to effectively develop and maintain partnerships and share cybersecurity-related information with federal and nonfederal entities to support its operation as required by the statutes.

Obtaining contact information of all owners and operators of the most critical cyber-dependent infrastructure assets. The National Cybersecurity Protection Act of 2014 requires NCCIC to facilitate cross-sector coordination to address cybersecurity risks and incidents. This includes cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors.

However, representatives of federal and nonfederal entities that own critical cyber assets that could have a catastrophic impact on the nation if victimized by a cyber attack were not fully represented in the NCCIC customer log.⁵⁴ Specifically, our review found that 23 percent of the entities owning such critical assets (as determined by DHS) were not represented within the master NCCIC customer log as of September 2016. Without representation of these entities, NCCIC may not have the information it needs readily available to facilitate coordination with critical asset owners. NCCIC officials were unable to demonstrate that they had a formal internal process for maintaining customer contact information and acknowledged that doing so remains a challenge for the center.

Without a concentrated effort on ensuring the full representation of the owners and operators of these critical assets, the center lacks assurance that it is adequately facilitating the cross-sector coordination of cybersecurity risk and incidents to the nation's most critical cyber-dependent assets that, if impacted, could have a catastrophic effect on the nation.

⁵⁴Section 9 of Executive Order 13636 directs the Secretary of Homeland Security to use a risk-based approach to identify critical infrastructure where a cybersecurity incident could result in catastrophic effects. Subsequently, the Secretary directed efforts that identified 65 cyber assets that met the criteria for a catastrophic affect if impacted by a cybersecurity incident.

Working across multiple network platforms. The National Cybersecurity Protection Act of 2014 requires NCCIC to coordinate the sharing of information across the government. This includes information related to cybersecurity risks and incidents.

However, we found that the sharing of information is complicated by NCCIC analysts having to operate across multiple networks, often manually entering data into each network, which decreases the rate of response of coordinating the sharing of incident information to customers and increases the risk of false entry. For example, officials stated that it takes on average 3 minutes for a ticket to be closed when working within one network. Across the 3 systems, it could take up to 15 minutes, depending on the size of the ticket, and the amount of information needed to be manually entered into each system.

According to senior NCCIC officials, this impediment was attributed to a legacy technical infrastructure implemented prior to the center's existence. They added that efforts were under way to address this impediment. However, NCCIC had not developed an implementation plan or established time frames for consolidating or integrating the networks.

Until NCCIC develops a process to avoid manual data entry, it will continue to face challenges in efficiently sharing information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents across the government.

Collaborating with international partners using the NCCIC Portal.

The Cybersecurity Act of 2015 requires NCCIC to engage with international partners, in consultation with other appropriate agencies, to (a) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and (b) enhance the security and resilience of global cybersecurity.

International and other partners have access to the center's products through the NCCIC Portal, which has functioned as a mechanism to disseminate products to recipients since 2003.⁵⁵ However, DHS is migrating the NCCIC portal to the Homeland Security Information Network. This network is categorized as a FIPS 199 high-impact system and, thus, requires authentication of individuals with access to the

⁵⁵Known as the US-CERT portal when it was established in 2003.

system. According to NCCIC officials, international partners had expressed a concern that the new network will have a negative impact on their collaboration with NCCIC because continued access would require the submission of international participants' passports and other sensitive personal information to a U.S. government entity.

While DHS has a responsibility to ensure the security over its high-impact systems, NCCIC may face a barrier to engaging with international partners. Without taking action to address this potential barrier, international partners may be reluctant to engage with NCCIC. Thus, the center may be challenged in its ability to collaborate and enhance global cybersecurity if it does not find alternative methods to engage and share information with international partners while ensuring the security requirements of high-impact systems.

Survey Respondents Varied in Their Reported Use of NCCIC Products and Services but Had Generally Favorable Views of the Center’s Activities

The respondents to our nongeneralizable survey of the center’s activities reported that they used its products and services to varying extents. The respondents also expressed generally favorable views of the center’s activities. Table 2 depicts the extent to which the survey respondents, who each self-identified as a customer of an NCCIC component (US-CERT, ICS-CERT, NCC, the Watch Floor, and NO&I), used, did not use, or were unsure if they used a particular NCCIC product or service.

Table 2: Nongeneralizable Survey Respondents’ Use of Products and Services Provided by National Cybersecurity and Communications Integration Center’s Components^a as a Percentage^b

Products and services			Used	Not Used	Unsure	Total number of respondents
<i>U.S. Computer Emergency Readiness Team (US-CERT) Products and Services</i>						
1.	Cyber Information Sharing and Collaboration Program (CISCP) Indicator Bulletins		71%	20%	10%	229
2.	US-CERT Indicator Bulletins		91%	6%	3%	250
3.	Malware Initial Findings Reports		65%	25%	10%	201
4.	Preliminary Digital Media Analysis Reports		24%	46%	30%	168
5.	Digital Media Analysis Reports		23%	52%	25%	164
6.	Malware Analysis Reports		59%	26%	15%	205
7.	Request for Information)		31%	48%	21%	193
8.	Victim/Abuse Notifications		19%	57%	24%	192
9.	Joint Analysis Reports		56%	30%	15%	196
10.	Joint Indicator Bulletins		64%	23%	13%	203

Products and services	Used	Not Used	Unsure	Total number of respondents
11. US-CERT Analysis Reports	80%	10%	10%	234
12. Customer and Partner Engagements (Conference Presentations)	53%	31%	16%	213
13. Vulnerability Information (i.e., MITRE: CVE, NVD, CERT Vulnerabilities)	81%	11%	7%	247
14. Incident Response Team Reports	36%	44%	20%	199
15. Incident Notifications	49%	37%	14%	219
<i>Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Products and Services</i>				
16. ICS Joint Working Group	60%	27%	13%	180
17. ICS Briefings	66%	24%	10%	174
18. ICS Reports	81%	13%	6%	184
19. ICS Classroom Training	37%	50%	13%	161
20. ICS Online Training	34%	51%	16%	148
21. ICS Cyber Assessments	35%	53%	12%	165
22. ICS Incident Response Deployment	16%	69%	14%	167
23. ICS Vulnerability Alerts	79%	16%	5%	178
<i>National Coordinating Center (NCC) Products and Services</i>				
24. Title Globe Communications Testing	14%	65%	21%	66
25. Shared Resources High Frequency Radio Program (SHARES)	16%	63%	22%	64
26. Emergency Support Function 2 Webinars and Videos	25%	54%	21%	67
27. Emergency Support Function 2 National Level Exercise Participation & Planning	23%	54%	23%	69
28. Emergency Support Function 2 Regional Exercise Participation	15%	58%	27%	67
29. NCC Watch Request for Information/Advisories/Situational Report	41%	35%	24%	68
30. NCC Watch Train Derailment Notifications	30%	49%	21%	71
31. Watch GPS Testing Notices	19%	60%	21%	68
32. NCC Watch Bulletin/Notifications - Other alerts	54%	25%	22%	69
33. NCC 0900 Monday Weekly Call	16%	61%	23%	62
34. NCC Event Infrastructure Analysis	25%	52%	23%	64
<i>Watch Floor Products and Services</i>				
35. Request for Information Response	55%	32%	13%	87
36. NCCIC Analysis Product (i.e., Weekly Analysis Synopsis Product)	75%	14%	11%	91
37. External Exercises	48%	38%	14%	86
38. National Level Exercises	58%	33%	9%	89
39. Tours	53%	39%	8%	87
40. Cyber Hygiene Scan Reports	45%	46%	9%	80
41. Watch Floor Situational Reports and Situational Assessments	49%	31%	19%	83

Products and services	Used	Not Used	Unsure	Total number of respondents
42. Information Sharing and Liaison Services	36%	52%	12%	89
43. Risk & Vulnerability Assessments	43%	45%	12%	86

Source: GAO analysis of survey responses. | GAO-17-163

Notes:

^aFor survey respondents who were aware that the particular product or service was provided by their self-identified component.

^bPercentages may not sum to 100 because of rounding.

With regard to evaluating the characteristics of products and services, the respondents to our nongeneralizable survey generally reported that NCCIC products and services were timely, relevant, and actionable. Specifically, 289 of 333 respondents (87 percent) found products and services they had used to be extremely, very, or moderately timely; 286 of 332 respondents (86 percent) found products and services to be extremely, very, or moderately relevant; and 234 of 332 respondents (70 percent) stated that products and services have led to an actionable result to a very great, great, or moderate extent (e.g., used to address a vulnerability or apply a defensive measure) on their part.

In addition, although between 12 and 18 percent of respondents to our nongeneralizable survey indicated a low level of effectiveness, respondents had generally favorable views of the center's provision of cybersecurity information. Specifically, 236 of 335 respondents (70 percent) evaluated the provision of cyber threat indicators to be at a high or moderate level of effectiveness. In addition, 219 of 333 respondents (66 percent) identified risks and incidents to be at a high or moderate level of effectiveness. Further, 211 of 339 respondents (62 percent) indicated cyber defensive information to be at a high or moderate level of effectiveness. Further, the survey respondents evaluated NCCIC's ability to provide timely, relevant, and actionable information at a 235 of 331 (71 percent), 245 of 334 (73 percent), and 222 of 339 (65 percent) high or moderate level of effectiveness, respectively.

Table 3 shows survey respondents' evaluations of NCCIC's effectiveness in providing them with cyber threat indicators, information on risks and incidents and defensive measures, and information that was timely, relevant, and actionable.

Table 3: Nongeneralizable Survey Respondents' Evaluation of the Effectiveness of National Cybersecurity and Communications Integration Center Activities as a Percentage^a

	High ^b	Moderate ^c	Low ^d	Don't know
Providing cyber threat indicators	44%	27%	13%	16%
Providing cybersecurity risks and incidents	39%	26%	15%	19%
Providing cyber defensive measures	34%	29%	14%	23%
Providing timely information	43%	28%	12%	17%
Providing relevant information	46%	28%	14%	13%
Providing actionable information	35%	30%	18%	17%

Source: GAO analysis of survey responses. | GAO-17-163

Notes:

^aPercentages may not sum to 100 because of rounding.

^bHigh designation represents the combination of responses that were "extremely" and "very" effective, timely, relevant, or actionable, as applicable.

^cModerate designation represents responses that were "moderately" effective, timely, relevant, or actionable, as applicable.

^dLow designation represents the combination of responses that were "slightly" or "not at all" effective, timely, relevant, or actionable, as applicable.

Survey respondents also evaluated the center's effectiveness with regard to its information sharing capability, the uniqueness in the information it provides, and its partnerships with them in improving the protection of critical cyber assets and functions, and how well it is fulfilling its mission. Table 4 shows respondents' overall evaluation of the center in terms of the effectiveness of its information sharing capability, customer partnerships, and the extent to which it is fulfilling its mission, among other things.

Table 4: Nongeneralizable Survey Respondents' Overall Evaluation of the National Cybersecurity and Communications Integration Center's Effectiveness in Carrying out of Its Mission as a Percentage^a

	High ^b	Moderate ^c	Low ^d	Don't know
Information sharing capability	46%	28%	12%	15%
Uniqueness of NCCIC information	35%	29%	17%	18%
Partnership with NCCIC in improving protection of entity critical cyber assets and function	38%	23%	17%	22%
NCCIC in fulfilling its mission as the cyber and communications integration center	45%	21%	10%	24%

Source: GAO analysis of survey responses. | GAO-17-163

Notes:

^aPercentages may not sum to 100 because of rounding.

^bHigh designation represents the combination of very great and great extent, extremely and very effective, as applicable, regarding the specific characteristics of NCCIC operations.

^cModerate designation represents moderate extent and moderately effective, as applicable, regarding the specific characteristics of NCCIC operations.

^dLow designation represents the combination of slight extent and no extent, slightly effective and not at all effective, as applicable, regarding the specific characteristics of NCCIC operations.

Further, respondents regarded NCCIC as important to the nation's ability to protect critical cyber assets and functions. Specifically, 264 of 337 respondents (78 percent) to our nongeneralizable survey stated that there would be a "very" or "somewhat" negative impact on the nation if the NCCIC products and services did not exist.

However, not all survey responses were positive. Specifically, survey respondents reported that they were not aware of all of the products and services that the center offered. The respondents added that they would be interested in receiving additional NCCIC products and services but were unsure about how to begin receiving them. The respondents reported that the center had not provided information identifying these products and services. NCCIC officials acknowledged that customers may not be aware of certain products and services because not all products and services are meant for every customer.

Conclusions

NCCIC, as the federal civilian cyber center, is generally performing 11 required cybersecurity functions through the development and dissemination of 43 products and services. However, the extent to which NCCIC carried out these cybersecurity functions in accordance with the 9 implementing principles is unclear. Until it determines the extent to which the implementing principles apply to these functions, NCCIC will not be able to fully assess the extent to which it is meeting the mandated principles. Further, without measuring the extent to which principles are being met, NCCIC will be challenged in articulating how effectively it is performing the functions in support of its role as a focal point for cybersecurity incident coordination, information sharing, and incident response across the federal civilian government and critical infrastructure.

NCCIC also faces several impediments that inhibits it from efficiently performing its cybersecurity functions. These impediments relate to consolidating entry points for receiving and logging potential incident data and maintaining the center's relationship with customers. Until NCCIC takes steps to overcome these impediments it may not be able to

efficiently perform its cybersecurity functions and assist federal and nonfederal entities in identifying cyber-based threats, mitigating vulnerabilities, and managing cyber risks.

Recommendations for Executive Action

To more fully address the requirements identified in the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015, we recommend that the Secretary of the Department of Homeland Security take the following nine actions:

1. Determine the extent to which the statutorily required implementing principles apply to NCCIC's cybersecurity functions.
2. Develop metrics for assessing adherence to applicable principles in carrying out statutorily required functions.
3. Establish methods for monitoring the implementation of cybersecurity functions against the principles on an ongoing basis.
4. Integrate information related to security incidents to provide management with more complete information about NCCIC operations.
5. Determine the necessity of reducing, consolidating, or modifying the points of entry used to communicate with NCCIC to better ensure that all incident tickets are logged appropriately.
6. Develop and implement procedures to perform regular reviews of customer information to ensure that it is current and reliable.
7. Take steps to ensure the full representation of the owners and operators of the nation's most critical cyber-dependent infrastructure assets.
8. Establish plans and time frames for consolidating or integrating the legacy networks used by NCCIC analysts to reduce the need for manual data entry.
9. Identify alternative methods to collaborate with international partners, while ensuring the security requirements of high-impact systems.

Agency Comments and Our Evaluation

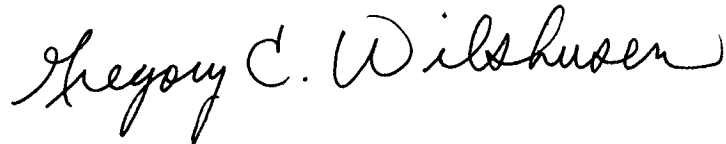
We received written comments on a draft of this report from DHS. In its comments, the department concurred with all nine recommendations. The department also provided details about steps that it plans to take to address each of the recommendations, including estimated time frames for completion. If effectively implemented, these actions should enhance the effectiveness and efficiency of NCCIC in performing its statutory

requirements. The department's written comments are reprinted in appendix V.

In addition to the aforementioned comments, DHS also provided a technical comment via e-mail, which we considered and incorporated.

We are sending copies of this report to the appropriate congressional committees, the Department of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive, flowing style.

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which the National Cybersecurity and Communications Integration Center (NCCIC) was performing its statutorily defined cybersecurity-related functions. To determine this, we analyzed two acts that establish roles and responsibilities for the center: the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015. These laws together require the center to carry out 11 cybersecurity functions. More specifically, the National Cybersecurity Protection Act of 2014 prescribed 7 functions and the Cybersecurity Act of 2015 prescribed 4 additional functions. The National Cybersecurity Protection Act of 2014 also identified 9 implementing principles. The two acts also contained provisions for GAO to report on NCCIC's implementation of its cybersecurity mission.

To determine the extent to which it was addressing the 11 cybersecurity functions, we analyzed the center's program descriptions, concepts of operations, and policies and procedures documenting how each of the center's components are to operate. For example, we analyzed the U.S. Computer Emergency Readiness Team (US-CERT) Strategic Action Plan, Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) Five-Year Plan (2015-2019), and the National Coordinating Center (NCC) Information Guide and Overview for 2015. In addition, we analyzed the NCCIC Watch Floor Concept of Operations that describes its operations. We corroborated information by interviewing center officials, including the Assistant Secretary for Cybersecurity and Communications, the Director of the NCCIC, and the directors of each of the center's components, as well as other responsible officials.

Based on our analysis of this information, we developed an initial list of products and services and held interviews with officials to confirm the total list of products and services. Based on these actions, we determined that the center develops and disseminates 43 products and services. We then collected and analyzed examples of each product and service to determine how they addressed each of the 11 cybersecurity functions established in the two laws. To gain a greater understanding of the purposes and methods of developing the products and services, we also interviewed NCCIC officials.

To identify instances where products and services addressed the 9 implementing principles, we analyzed relevant program documentation and reviewed the procedures by which the center develops its products and services. We corroborated our information by interviewing NCCIC officials responsible for product and service development. To gain a greater understanding of its operations, we visited the site of the ICS-

CERT operations in Idaho Falls, Idaho, to observe its activities, including the development of its products and services. We also observed operations of the Watch Floors in Arlington, Virginia and Idaho Falls, Idaho, and interviewed officials responsible for operating the Watch Floors, developing services, and liaising with federal and nonfederal partners.

We also analyzed the dissemination methods of products and services by examining the contents of the NCCIC web portal, including how the customer base was segmented to disseminate products and services in accordance with information sharing protections. At the ICS-CERT facility in Idaho Falls, Idaho, we observed the basic ICS training exercise services provided to customers. We also collected and analyzed performance measures and interviewed officials about the actions being taken to improve its measurement efforts and efforts to consolidate operations across NCCIC components. In addition, NCCIC officials provided budget execution information that we analyzed to determine the reported amount spent across three fiscal years for each component. During the interviews, we discussed with officials the impediments that the center faced in more efficiently performing the 11 cybersecurity functions.

To obtain the views of the recipients of the center's products and services, we administered a survey to a sample of individuals identified by NCCIC as having access to a product or service, or participating in a center group or activity. We asked customers about their awareness and use of the 43 products and services, and other activities and roles performed by the center. We then asked them to assess their experiences, including rating the effectiveness and the implementing principles of timeliness, actionability, and relevance. We also asked respondents to rate various elements of NCCIC in terms of importance, expectations, challenges, and reasons for not using the center's products and services.

To develop our questionnaire, we met with NCCIC officials and identified the activities performed for customers, including the development and dissemination of 43 products and services, disseminated to customers. We pretested draft versions of the questionnaire with nonfederal representatives of two Information Sharing and Analysis Centers and an information security officer at a federal agency, to reflect some of the variation in the population.

We defined the target population for the survey to be all organizational points of contact or other individuals identified by NCCIC, as of June 8, 2016, as having access to a product or service, or participating in a center group or activity. NCCIC provided us with 19,573 records across 14 lists of customer contact information. Some of the provided lists consisted only of e-mail addresses of individuals subscribed to a particular NCCIC product or service, while others consisted of members of a group. Some organizations were represented by many individual e-mail addresses across the lists, and some individuals appeared on more than one list. While the basic unit of the population to be sampled was an individual e-mail address, due to the variability in coverage of the population mentioned above, an individual survey respondent may be representing their own personal experiences and opinions, or those of an organization, and multiple respondents may be representing the same organization.

After removing records with missing, incomplete, or erroneously duplicative e-mail addresses within each list, our sample was reduced to 19,293 records. We did not remove multiple instances of the same e-mail address appearing on more than one list; these duplicates were retained in the sample frame so that each instance of that e-mail address might have a chance of initial selection proportional to the size of the customer list it appeared on.

We initially drew a random but nongeneralizable sample of 2,907 e-mail address records, allocated across the 16 customer types roughly proportional to the sizes of each type. We then removed 115 of this initial sample because their e-mail addresses duplicated selections made from other customer lists, for a total sample of 2,792 customer records with unique e-mail addresses, which we attempted to contact with our survey.

We began our survey on August 2, 2016. We sent e-mails with login information to the web-based questionnaire to the sample. We sent up to three follow-up e-mails during the fieldwork period to those who had not yet responded. The survey ended on September 8, 2016. The outcomes of the survey fieldwork are displayed in table 5 below.

Table 5: Outcomes of GAO's National Cybersecurity and Communications Integration Center Customer Survey Sample

Outcome	Number
Usable response	340
Partial but unusable response	114

Outcome	Number
Refusal to respond	3
Other nonresponse	2,032
Ineligible – not in population (nonworking e-mail address, recipient no longer at organization, Department of Homeland Security/NCCIC employee)	303
Total sample fielded	2,792

Source: GAO analysis of survey responses and data. | GAO-17-163

The response rate to the survey, calculated as the number of usable responses divided by the number found to be eligible was about 14 percent. Because of the variability in coverage of the population by the sample frame, irregularities in the contact information and eligibility of the records sampled, and the low rate of response to the survey, the results of this survey only represent those that responded, and are not generalizable to any larger population of NCCIC customers. We do not make any inferences about those not sampled or not responding to the survey.

In addition to this limitation, questionnaire surveys of this kind are subject to other potential errors. To minimize the possibility of measurement error (differences between reported and true answers) arising from question design, interpretation or administration, or the misreporting of answers, we designed and administered the survey in consultation with survey methodologists, made improvements to the questionnaire based on pretest results, and had a separate survey methodologist review the draft questionnaire to identify potential problems in questionnaire design.

Of the 340 respondents, 14 percent identified themselves as individual participants in NCCIC activities, 64 percent as representatives of a single public or private organization, 13 percent as representing an association or other entity representing a sector or group of organizations, and 9 percent identified in other ways. Thirty-four percent said they represented federal government entities; 18 percent said they represented state, local, or tribal entities; 44 percent said they represented private sector entities; and 4 percent gave other answers.

During the processing and analysis of reported data, we also identified and corrected for patterns of response across questions that we could identify as inconsistent or contradictory. Nonresponse error (failure to obtain a response to a question or the questionnaire) may lead to bias in the results if those who do not respond would have given materially different responses from those who did respond. To minimize

nonresponse, we made follow-up contacts throughout the survey. To minimize *processing error* (mistakes in converting reported data into published survey results), data processing and analysis programming was independently verified by a separate data analyst.

We conducted this performance audit from January 2016 to February 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: NCCIC Product and Service Information

Table 6 below highlights the total number of each product and service that the National Cybersecurity and Communications Integration Center (NCCIC) reported providing to its customers in fiscal years 2015 and 2016.

Table 6: Number of National Cybersecurity and Communications Integration Center (NCCIC) Products and Services Produced or Performed in Fiscal Years 2015 and 2016

Product or Service	Description	Total number issued for fiscal year 2015	Total number issued for fiscal year 2016
<i>Component: U.S. Computer Emergency Readiness Team (US-CERT)</i>			
1. Cyber Information Sharing and Collaboration Program (CISCP) Indicator Bulletins	Provides incident analysis information derived from new cyber incidents and/or malicious code, threats, and vulnerabilities to CISC partners including local and state government, critical Infrastructure , private industry, or a country CERT.	235	218
2. US-CERT Indicator Bulletins	A short turnaround bulletin containing threat-specific indicators of compromise.	137	151
3. Malware Initial Findings Reports	Preliminary analysis and initial mitigation recommendations for submitted malware artifacts.	165	114
4. Preliminary Digital Media Analysis Reports	Reports of initial findings from a forensic investigation of digital media.	15	13
5. Digital Media Analysis Reports	Reports of full forensic analysis of digital media.	16	2
6. Malware Analysis Reports	Reports containing full analysis, indicators of compromise, tactics, techniques, and procedures and mitigation recommendations for submitted malware artifacts.	38	37
7. Request for Information	A request made by a third party for information, or more information, on either general cybersecurity issues or specific incidents or issues of interest to the requestor.	1360	1278
8. Victim/Abuse Notifications	A victim notification is sent to a third party based on information that they may be a victim of a cybersecurity event. An abuse notification is sent to a third party based on information that they may have systems that are being used for malicious purposes.	No data provided	No data provided
9. Joint Analysis Report	An analysis report produced in coordination with US-CERT's trusted partners (i.e. law enforcement or Intelligence community).	3	5
10. Joint Indicator Bulletins	An indicator bulletin produced in coordination with US-CERT's trusted partners (i.e. law enforcement or Intelligence Community).	6	1
11. US-CERT Analysis Reports	Provides indicators of compromise and tactics, techniques, and procedures related to specific threats.	11	3

Appendix II: NCCIC Product and Service Information

Product or Service	Description	Total number issued for fiscal year 2015	Total number issued for fiscal year 2016
12. Customer and Partner Engagements (Conference Presentations)	US-CERT's efforts to build and leverage partnerships across the federal government; state, local, tribal, and territorial governments; the private sector; and the international community. Enhancing trust through customer and partner engagement is critical to enabling greater information sharing and improving coordination about cyber events.	No data provided	No data provided
13. Vulnerability Information	Provides information about software vulnerabilities, including summaries, technical details, remediation information, and lists of affected vendors. Many vulnerability notes are the result of private coordination and disclosure efforts.	14,425	6,494
14. Incident Response Team Reports	A report provided to external customers on the impact of a particular compromise. For example, officials stated that their activities to assist the Office of Personnel Management during its information breach would fall under this product. An output of this product would be a report to the affected party. Other outputs of this product may result in binding operational directives to agencies, or information for OMB memoranda.	15	23
15. Incident Notifications	US-CERT detects malicious cyber activity targeting federal agencies through tools such as EINSTEIN.	536	757
<i>Component: Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)</i>			
16. ICS Joint Working Group	A collaborative and coordinating body that provides a vehicle for communicating and partnering across all Critical Infrastructure (CI) Sectors between federal agencies and departments, as well as private asset owners/operators of industrial control systems.	1	2
17. ICS Briefings	Briefings provided in small group or large group formats discussing ICS-CERT and current threats, actions and products.	343	343
18. ICS Reports	Reports on cyber activity related to critical infrastructure on current threats, actions to take and defensive measures.	332	273
19. ICS Classroom Training	Technical training about security control systems that are provided in person either at an entity or through individual sign-up.	1,300	1,614
20. ICS Online Training	Online training modules with a blended learning approach, which makes accessing course material easier and more efficient, reduces redundancy in training materials, and eliminates the need to travel to participate in ICS-CERT training.	3,500	15,156

Appendix II: NCCIC Product and Service Information

Product or Service	Description	Total number issued for fiscal year 2015	Total number issued for fiscal year 2016
21. ICS Cyber Assessment	Assessments include a Design Architecture Review (DAR), a technical review and cyber evaluation of ICS operations; a Cybersecurity Evaluation Tool, a basic one day assessment ending in a report on the organization's cyber posture; and a Network Architecture Verification and Validation (NAVV), where DHS uses tools to review and analyze network traffic occurring within the ICS network.	112	117
22. ICS Incident Response Deployment	Incident response assistance either on-site or remote and incident analysis that varies based upon the nature of the cybersecurity incident.	5	3
23. ICS Vulnerability Alerts	An alert provided from ICS-CERT indicating a vulnerability identified and what actions an entity can take to mitigate the vulnerability, including implementing a patch.	27	23
<i>Component: National Coordinating Center (NCC)</i>			
24. Title Globe Communications Testing	A monthly test of the communications capabilities of federal departments and agencies. The results of the tests are provided to each entity, with quarterly reports sent to the White House.	12	12
25. Shared Resources High Frequency Radio Program	Testing of the over 1600 high-frequency radio stations across the country that have agreed to pass federal traffic in times of crisis. It is meant to be a contingency communication system when other communications go out.	No data provided	1,682
26. Emergency Support Function 2 Webinars and Videos	Online resources for training and knowledge management related to Emergency Support Function 2.	10	6
27. Emergency Support Function 2 National Level Exercise Participation & Planning	Activities related to national level exercises to support Emergency Support Function 2.	5	5
28. Emergency Support Function 2 Regional Exercise Participation	Exercises to test regional communication infrastructures related to Emergency Support Function 2.	0	4
29. NCC Watch Request for Information (RFI)/Advisories/Situational Report (SITREP)	An RFI is produced to identify impacts or concerns from government and/or industry partners. An RFI is supplemented with an Advisory summarizing the responses received from the RFI. A SITREP is produced when an incident will require additional reporting.	70	72
30. NCC Watch Train Derailment Notifications	Notification of communications disruption disseminated to government and industry partners, as a result of an incident identification from the Department of Transportation Crisis Management Center.	283	297
31. Watch GPS Testing Notices	Notification of a scheduled test in a geographical area to determine if there are equipment malfunctions or external problems (e.g. natural disaster) with a communications medium.	116	117
32. NCC Watch Bulletin/Notifications	Other alerts.	358	247

Appendix II: NCCIC Product and Service Information

Product or Service	Description	Total number issued for fiscal year 2015	Total number issued for fiscal year 2016
33. NCC 0900 Monday Weekly Call	Operations round table to discuss situation awareness with members of the communications infrastructure.	47	46
34. NCC Event Infrastructure Analysis	An assessment of communications in a specific area that is either supportive or could be affected by the scheduled event.	24	18
<i>Component: NCCIC Watch Floor</i>			
35. Request for Information Response	An entity requests information from NCCIC and the Watch Floor responds if it can and/or it provides the request to the appropriate NCCIC component.	189	918
36. NCCIC Analysis Product (i.e. Weekly Analysis Synopsis Product)	NCCIC analysis products for special events (e.g. the Super Bowl) or malware.	13	6
37. External Exercises	Exercises that include federal, state local tribal, territorial, private, and international partners and range from individual table-top exercises to multi-organization exercises. Other examples are when NCCIC is asked to teach an entity how to conduct exercises, manage a cyber exercise or provide analysis on an exercise already completed.	45	58
38. National Level Exercises	Exercises that are longer and orders of magnitude more costly than a regular exercise and include thousands of participants. Examples include Cyberstorm and Cyberguard.	2	3
39. Tours	Classified and unclassified tours of the NCCIC floor including an operations briefing on how NCCIC accomplishes its mission.	286	239
40. Cyber Hygiene Scan Reports	Automated weekly reports for customers who requested NCCIC to continuously scan for vulnerabilities.	4,928	12,187
41. Watch Floor Situational Reports and Situational Assessments	Reports delivered after an incident has occurred based on what NCCIC knows and does not know regarding the incident. Reports are tailored for specific sectors and may be updated when further analysis has been conducted by NCCIC.	16	22
42. Information Sharing and Liaison Services	Vehicles by which federal and nonfederal entities are able to become a part of the NCCIC watch floor, such as Memoranda of Agreement or Cooperative Research and Development Agreements.	No data provided	118
43. Risk & Vulnerability Assessments	Penetration testing requested from an entity that provides the entity with knowledge on how to harden their security and identify the signs that an attacker is on their network.	48	117

Source: GAO Analysis of Department of Homeland Security data | GAO-17-163

Appendix III: NCCIC Products and Services Supporting Cybersecurity Functions

The National Cybersecurity and Communications Integration Center (NCCIC) is required to perform 11 cybersecurity functions. Table 7 below summarizes how the 43 products and services were being used as of October 2016 in support of the 11 functions.

Table 7: National Cybersecurity and Communications Integration Center Products and Services Used in Performing Prescribed Functions, as of October 2016

Product or Service	Functions										
	1 ^a	2 ^b	3 ^c	4 ^d	5 ^e	6 ^f	7 ^g	8 ^h	9 ⁱ	10 ^j	11 ^k
1. Cyber Information Sharing and Collaboration Program Indicator Bulletins	X		X	X	X						
2. U.S. Computer Emergency Readiness Team (US-CERT) Indicator Bulletins	X	X	X		X						
3. Malware Initial Findings Reports								X	X		
4. Preliminary Digital Media Analysis Reports							X		X		
5. Digital Media Analysis Reports							X		X		
6. Malware Analysis Reports									X		
7. Request for Information	X							X			
8. Victim/Abuse Notifications		X	X					X			
9. Joint Analysis Report	X		X								
10. Joint Indicator Bulletins	X		X								
11. US-CERT Analysis Reports		X			X						
12. Customer and Partner Engagements							X	X			
13. Vulnerability Information					X		X	X			
14. Incident Response Team Reports						X	X				
15. Incident Notifications		X		X							
16. Industrial Control Systems (ICS) Joint Working Group				X							
17. ICS Briefings			X				X	X			
18. ICS Reports	X		X				X	X			
19. ICS Classroom Training							X				
20. ICS Online Training							X				
21. ICS Cyber Assessments						X	X				
22. ICS Incident Response Deployment		X				X	X				
23. ICS Vulnerability Alerts					X		X	X			
24. Title Globe Communications Testing				X			X				
25. Shared Resources High Frequency Radio Program (SHARES)							X				

**Appendix III: NCCIC Products and Services
Supporting Cybersecurity Functions**

Product or Service	Functions										
	1 ^a	2 ^b	3 ^c	4 ^d	5 ^e	6 ^f	7 ^g	8 ^h	9 ⁱ	10 ^j	11 ^k
26. Emergency Support Function 2 Webinars and Videos							X				X
27. Emergency Support Function 2 National Level Exercise Participation & Planning										X	X
28. Emergency Support Function 2 Regional Exercise Participation										X	X
29. National Coordinating Center (NCC) Watch Request for Information /Advisories/ Situational Report		X			X						
30. NCC Watch Train Derailment Notifications		X									
31. Watch GPS Testing Notices		X									
32. NCC Watch Bulletin/Notifications - Other alerts		X									
33. NCC 0900 Monday Weekly Call				X							X
34. NCC Event Infrastructure Analysis		X									
35. Request for Information Response	X										
36. NCCIC Analysis Product (i.e., Weekly Analysis Synopsis Product)		X	X		X		X				
37. External Exercises										X	
38. National Level Exercises								X		X	
39. Tours	X							X			
40. Cyber Hygiene Scan Reports						X					
41. Watch Floor Situational Reports and Situational Assessments		X			X						
42. Information Sharing and Liaison Services	X		X	X							
43. Risk & Vulnerability Assessments						X					
Total products or services addressing each function	9	12	9	6	8	5	16	10	4	4	4

Source: GAO analysis of Department of Homeland Security, National Cybersecurity and Communications Integration Center products and services. | GAO-17-163.

^aFunction 1: Be a federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis and warnings for federal and nonfederal entities.

^bFunction 2: Provide shared situational awareness to enable real-time, integrated, and operational actions across the federal government and nonfederal entities to address cybersecurity risks and incidents to federal and nonfederal entities.

^cFunction 3: Coordinate the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks and incidents across the federal government.

^dFunction 4: Facilitate cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors.

^eFunction 5: Conduct and share integration and analysis, including cross-sector, of cyber threat indicators, defensive measures, cybersecurity risks and incidents with federal and nonfederal entities.

**Appendix III: NCCIC Products and Services
Supporting Cybersecurity Functions**

^fFunction 6: Provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks and incidents, which may include attribution, mitigation, and remediation.

^gFunction 7: Provide information and recommendations on security and resilience measures to federal and nonfederal entities, including information and recommendations to facilitate information security and strengthen information systems against cybersecurity risks and incidents; and share cyber threat indicators and defensive measures.

^hFunction 8: Engage with international partners, in consultation with other appropriate agencies, to (a) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and (b) enhance the security and resilience of global cybersecurity.

ⁱFunction 9: Share cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with federal and nonfederal entities, including across sectors of critical infrastructure and with state and major urban area fusion centers, as appropriate.

^jFunction 10: Participate, as appropriate, in national exercises run by the Department of Homeland Security (DHS).

^kFunction 11: Coordinate with the Office of Emergency Communications within DHS, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

Appendix IV: Examples of How NCCIC Products and Services Address the Implementing Principles

Although the National Cybersecurity and Communications Integration Center (NCCIC) did not completely determine the applicability of statutory implementing principles to its products and services, table 8 below provides examples of our determination of how NCCIC products and services adhered to the principles.

Table 8: Sample of Product and Services that Demonstrate How the National Cybersecurity and Communications Integration Center (NCCIC) Adhere to the Implementing Principles

Principle	Description
1. Ensure that the information is timely, actionable, and relevant to risks, incidents, and analysis shared	<p>NCCIC has general guidelines for developing and disseminating information to its customers. However, for a several products and services, there are no established measures to determine the timeliness, actionability, and relevancy, where applicable. For example, according to officials responsible for conducting Risk and Vulnerability Assessments, the service has an estimated completed timeframe of 8-10 weeks for each customer. This includes 6-8 weeks of off-site discussion with the customer in addition to 2 weeks of focused testing and review. However, these time frames are not established metrics by which officials evaluate the timeliness of that service. Further, Incident Notifications, derived from a notification of malicious activity from an EINSTEIN sensor at one of the participating federal agencies, requires a U.S. Computer Emergency Readiness Team (US-CERT) analyst to develop a network analysis report. According to DHS officials, these reports are generally responded to within 30 minutes; however this is not an established timeliness metric by which they evaluate the timeliness of the Incident Notification.</p> <p>With respect to ensuring relevance, during the development of NCCIC Analysis Products, an official reviews open source information pertaining to new malware or vulnerabilities and determines the most relevant information to be included. Officials disseminate this product, which includes recommendations directed to mitigate risks.</p>
2. Ensure that when appropriate, information related to risks, incidents, and analysis is integrated with other information and tailored to a sector	<p>Incident information is used in the development of its products to be disseminated to sectors. For example, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) holds briefings with, and provides compiled reports to, the industrial control community, across multiple sectors. These reports contain information relative to ongoing threats the ICS community faces. In addition, US-CERT Analysis reports integrate information related to cybersecurity risks and are disseminated to customers across multiple sectors or are, when applicable, tailored for those within a specific sector.</p> <p>Further, NCCIC conducts Situational Assessments and Advisories that integrate information related to risks, incidents, and analyses to be disseminated to a sector. For example, NCCIC disseminated information related to a ransomware incident to its federal partners. In another example, NCCIC disseminated integrated information regarding Tropical Storm Hermine to its Communications Infrastructure Information Sharing and Analysis Center partner.</p> <p>However, this principle may not be applicable to some products and services such as Cyber Hygiene assessments or Risk and Vulnerability assessments, as those services disseminate related risks specifically to federal agencies and customers who voluntary request those services.</p>

**Appendix IV: Examples of How NCCIC
Products and Services Address the
Implementing Principles**

Principle	Description
3. Ensure that the activities are prioritized and conducted based on the level of risk	<p>NCCIC uses its Cyber Incident Scoring System (NCISS) to evaluate risk for incidents directed to the Watch Floor as Requests for Information. The incidents are scored based on the system and assigned a level commensurate with priority for remediation.</p> <p>NCISS uses a weighted arithmetic mean to produce a score from zero to 100. This score drives NCCIC incident triage and escalation processes and assists in determining the prioritization of limited incident response resources and the necessary level of support for each incident. However, the system is not currently designed to support cases where multiple correlated incidents may increase overall risk, such as multiple simultaneous compromises of organizations in a specific sector or region. After an incident is scored, it is assigned a priority level. The six levels are aligned with NCCIC, the Department of Homeland Security (DHS), and the Cyber Incident Severity Schema (CISS) to help provide a common lexicon when discussing incidents. This priority assignment drives NCCIC urgency, pre-approved incident response offerings, reporting requirements, and recommendations for leadership escalation.</p>
4. Ensure that industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration	<p>In its capacity to develop and disseminate vulnerability alerts through the National Vulnerability Database, NCCIC works with contacts with industry, academia, and National Laboratories. More specifically, NCCIC works with members from industry manufacturers, such as Siemens and General Electric and contacts from various institutions such as the University of Alabama, University of Nebraska at Omaha, Iowa State University, and University of California in coordinating the development and dissemination of vulnerability alerts. NCCIC also works with customers from the Idaho National Laboratory and the Pacific Northwest National Laboratory to develop and disseminate vulnerabilities related to industrial control systems.</p>
5. Ensure that continuous, collaborative, and inclusive coordination occurs across sectors, with sector coordination councils, information sharing and analysis organizations and other nonfederal partners	<p>NCCIC facilitates inclusive collaboration through the NCCIC Watch Floor, which enables direct access to liaison officers and embedded staff from partner organizations. These organizations include representatives from other federal agencies, components of DHS, the private sector as well as state and local. NCCIC provides in-person classified and unclassified tours of the Watch Floor and also provides its customers with a vehicle to establish a temporary residence on the Watch Floor. NCCIC also facilitates a weekly teleconference with private and public entities, including the Communications Information Sharing and Analysis Center (ISAC), to discuss situational awareness and ongoing informational analysis related to current events, such as Train Derailments and Vulnerabilities.</p>
6. Ensure that as appropriate, the Center works to develop and use mechanisms for sharing information related to cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient	<p>NCCIC uses a variety of commonly used technology products, such as e-mail, Microsoft Office Applications, and portable document format (PDF) to disseminate information. For example, to disseminate reports related to the NCCIC's assessment services including the ICS Cyber Assessments, NCCIC provides its customers reports with findings and mitigation recommendations to be addressed. For responding to Requests for Information, NCCIC uses e-mail services to communicate with its partners, and its customers regarding incidents and situational assessments. NCCIC also uses an Internet Portal to disseminate its products to its customers.</p>

**Appendix IV: Examples of How NCCIC
Products and Services Address the
Implementing Principles**

Principle	Description
7. Ensure that it works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents	Joint Indicator Bulletins and Joint Analysis are examples of products developed in collaboration with other agencies, such as the Federal Bureau of Investigation, as a means to minimize duplicative sharing. However, for other products and services, this principle would not apply. Specifically, the Incident Response Team reports are developed after at least two weeks of onsite incident response. The output would contain the findings of the onsite activity, with information on the impacts of the compromise. As such, the report would only be delivered to the submitting entity and not vetted with any other federal agency.
8. Ensure that the information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access	NCCIC uses the Traffic Light Protocol (TLP) which is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four color designations to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s) for its products and services. For example, TLP: White indicates information that is without restriction, subject to copyrights, while TLP: Red indicates information that should not be shared outside of the intended exchange. NCCIC disseminates its products via the NCCIC portal using TLP protections for products such as Indicator Bulletins, Analysis Reports, Malware Initial Findings Reports, and Malware Analysis Reports.
9. Ensure that activities conducted comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons.	NCCIC has developed policies and guidelines to direct activities to be compliant with policies, regulations, and laws that protect the privacy and civil liberties of United States persons. For example, DHS released policies related to sharing cyber threat indicators and defensive measures and guidelines associated with ensuring privacy and civil liberties. In addition, DHS issued a policy relating to sharing cyber threat indicators and defensive measures which requires protection of threat indicators in accordance with the Cybersecurity Information Sharing Act of 2015. DHS also issued guidance to assist nonfederal entities to share cyber threat indicators and defensive measures, which describes the identification of types of information that would be a threat indicator even without items such as personal information. In conducting its activities to disseminate its products and services, NCCIC leverages its portal to apply sharing designations limiting the disclosure of private information. For example, to conduct Risk and Vulnerability assessments and Cyber Hygiene assessments, NCCIC adopts rules of engagement with the entity that includes a reference to laws and policies.

Source: GAO analysis of Department of Homeland Security data. | GAO-17-163.

Appendix V: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

January 18, 2017

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-17-163, "CYBERSECURITY:
DHS's National Integration Center Generally Performs Required Functions but
Needs to Evaluate Its Activities More Completely"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing the report.

The Department is pleased to note GAO's highlighting of the key accomplishments and importance of the National Cybersecurity and Communications Integration Center (NCCIC) as it relates to the National Cybersecurity Protection Act of 2014 and Cybersecurity Act of 2015. Specifically, the draft report recognizes DHS for completing 24 required actions outlined in the statutes by the specific due dates. It also acknowledges the NCCIC's development and dissemination of products and services that correspond to the 11 statutorily defined functions prescribed in the statutes. Additionally, DHS appreciates GAO's decision to survey NCCIC customers and share their valuable feedback, which demonstrates that the respondents place a high level of importance on the NCCIC as a source of cyber threat indicators, risks and incidents, and cyber defense information.

DHS remains committed to protecting our Nation's critical infrastructure from physical and cyber threats. Cyberspace has united once distinct information structures, including our business and government operations, our emergency preparedness communications, and our critical digital and process control systems and infrastructures. Protecting these systems is essential to the resilience and reliability of the Nation's critical infrastructure and key resources; therefore, to our economic and national security. The NCCIC is critical to these efforts.

The draft report contained nine recommendations with which the Department concurs. Attached find our detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

**Attachment: DHS Management Response to Recommendations
Contained in GAO-17-163**

GAO recommended that the Secretary of the Department of Homeland Security:

Recommendation 1: Determine the extent to which the statutorily required implementing principles apply to NCCIC's cybersecurity functions.

Response: Concur. The Department acknowledges that the statutorily required principles are critical to the successful execution of the cybersecurity mission. The National Protection and Programs Directorate's (NPPD) Assistant Secretary for Cybersecurity and Communications (CS&C) is currently reviewing all functions with the goal of identifying the most critical improvement opportunities in the areas identified in the statute, such as control of classified information, incorporation of private sector expertise, and actionability by stakeholders. Areas identified for improvement will be further analyzed, measured and evaluated. Additional details regarding these reviews are provided in our responses to Recommendations 2 and 3, as noted below. Estimated Completion Date (ECD): March 31, 2017.

Recommendation 2: Develop metrics for assessing adherence to applicable principles in carrying out statutorily required functions.

Response: Concur. In an ever-changing cyber environment, continuous improvement and measuring of the effectiveness of our products and services is essential. Once mapping of the implementing principles has been completed, NPPD's Assistant Secretary for CS&C will develop measurements of effectiveness (MOE) against the appropriate implementing principles, while conforming to Government Performance and Results Modernization Act requirements. In addition, NCCIC will take a phased approach to implementing performance measures to ensure sufficient sampling is done and baselines have been established. ECD: September 30, 2017.

Recommendation 3: Establish methods for monitoring the implementation of cybersecurity functions against the principles on an ongoing basis.

Response: Concur. In concert with Recommendations 1 and 2, NPPD's Assistant Secretary for CS&C will monitor the implementation of cybersecurity functions against established principles. Once applicable principles have been identified and mapped to NCCIC products and services, NPPD will implement a continuous review and improvement process in order to ensure the functions and principles remain aligned. ECD: September 30, 2017.

Recommendation 4: Integrate information related to security incidents to provide management with more complete information about NCCIC operations.

Response: Concur. The integration of numerous classified and unclassified information sources into a common operating picture is a primary function of the NCCIC. In this regard, the effective and efficient operation of the NCCIC relies on the ability to integrate, as well as the ability to manage and present information to senior leadership for operations execution and for resource planning. NPPD's Assistant Secretary for CS&C is working to improve the incident management process and the integration of systems currently managing security incident information. Integrating incident information across classified and unclassified networks is a continuing challenge, but the NCCIC continues to partner with other cyber centers to identify best practices for information management. NCCIC is currently updating its security guidelines, which will include appropriate best practices, as appropriate. ECD: November 30, 2017.

Recommendation 5: Determine the necessity of reducing, consolidating, or modifying the points of entry used to communicate with NCCIC to better ensure that all incident tickets are logged appropriately.

Response: Concur. DHS recognizes the challenges in handling a multitude of incidents from public and private customers. Integrating the incident ticketing management systems may result in a more streamlined and efficient approach for meeting mission requirements. Concurrently, NPPD's Assistant Secretary for CS&C is exploring the feasibility and impact of integrating the ticketing management systems which will require multiple levels of coordination. NPPD's external coordination will focus on NCCIC stakeholders to ensure mission needs can be met more effectively and efficiently while using a single, integrated system. Internal coordination efforts will focus on developing and documenting standardized ticketing management procedures within the Department through a collaborative process between NCCIC leadership, NPPD's Chief Financial Officer, Program and Evaluation Branch, and the Chief Information Officers from both NPPD and DHS. The goal of this effort will be to assess the feasibility, impact, overall IT implementation costs, resourcing and other program requirements. ECD: November 30, 2017.

Recommendation 6: Develop and implement procedures to perform regular reviews of customer information to ensure that it is current and reliable.

Response: Concur. The NCCIC recognizes the benefits of maintaining a complete and accurate inventory of a large customer base and strives to inform its customers through many outreach activities and access points for information about the portal, NCCIC's website, and extensive use of social media. NPPD's Assistant Secretary for CS&C is developing procedures and guidance for all components to use that will improve the accuracy of NCCIC's well-informed customer inventory. ECD: October 30, 2017.

4

Recommendation 7: Take steps to ensure the full representation of the owners and operators of the nation's most critical cyber-dependent infrastructure assets.

Response: Concur. NPPD has improved its relationship with key critical infrastructure asset owners by integrating the customer engagement functions, which enhances the overall relationships between asset owners and the Department. NPPD's Assistant Secretary for CS&C will develop an action plan to ensure these relationships are managed appropriately. ECD: November 30, 2017.

Recommendation 8: Establish plans and time frames for consolidating or integrating the legacy networks used by NCCIC analysts to reduce the need for manual data entry.

Response: Concur. The NCCIC was initially created by consolidating several components with significant prior investment in information technology. Integrating networks, applications and data has been a significant portion of the NCCIC's mission. It is important to note that due to security classification requirements not all information systems can be directly integrated. NPPD's Assistant Secretary for CS&C will develop plans and timeframes for consolidating or integrating information systems, as appropriate, including a review and benchmarking of classified information integration practices at other cyber centers for applicability to NCCIC networks. ECD: April 30, 2017.

Recommendation 9: Identify alternative methods to collaborate with international partners, while ensuring the security requirements of high-impact systems.

Response: Concur. International partners currently have access to NCCIC information sharing products through the NCCIC Portal (formerly US-CERT portal), which has been NPPD's tool to disseminate products since 2003. DHS is migrating the NCCIC Portal to the Homeland Security Information Network (HSIN) in fiscal year 2017, which will require authentication of all individuals with access to the system. International partners have expressed concerns that the new network will have a negative impact on their collaboration with the NCCIC because continued access would require the submission of sensitive personal information to the U.S. Government. We recognize that migrating to the HSIN may impact coordination with international partners, and are exploring alternative methods for sharing information while maintaining access control. NPPD's Assistant Secretary for CS&C will closely monitor the new security policies associated with the HSIN migration in order to identify negative impacts to the NCCIC's operational mission and coordination with international partners. ECD: June 30, 2017.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, Michael W. Gilmore (assistant director), Kush K. Malhotra (analyst in charge), Chris Businsky, Lee A. McCracken, Constantine Papanastasiou, David Plocher, Carl Ramirez, and Priscilla A. Smith made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [LinkedIn](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.